

PCT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room 524
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 26 October 2000 (26.10.00)	
International application No. PCT/GB00/00495	Applicant's or agent's file reference 30990085 WO
International filing date (day/month/year) 15 February 2000 (15.02.00)	Priority date (day/month/year) 15 February 1999 (15.02.99)
Applicant CHEN, Liqun et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

15 September 2000 (15.09.00)

☐ in a notice effecting later election filed with the International Bureau on:2. The election ☒ was☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Zakaria EL KHODARY
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

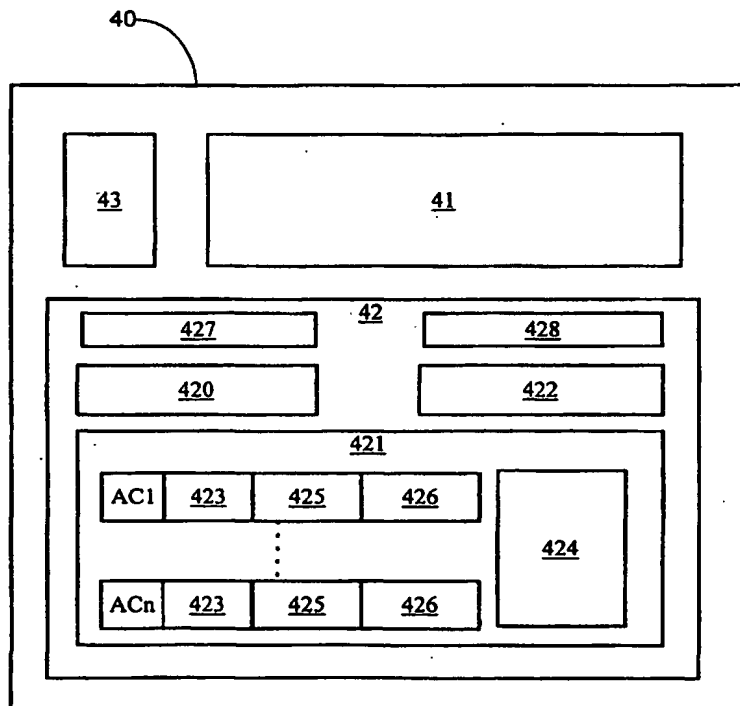


INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : G06F 1/00, 11/22	A1	(11) International Publication Number: WO 00/48061 (43) International Publication Date: 17 August 2000 (17.08.00)
(21) International Application Number: PCT/GB00/00495 (22) International Filing Date: 15 February 2000 (15.02.00) (30) Priority Data: 99301100.6 15 February 1999 (15.02.99) EP 9922663.1 25 September 1999 (25.09.99) GB (71) Applicant (for all designated States except US): HEWLETT-PACKARD COMPANY [US/US]; 3000 Hanover Street, Palo Alto, CA 94304 (US). (72) Inventors; and (75) Inventors/Applicants (for US only): CHEN, Liqun [CN/GB]; 1 Harvest Close, Bradley Stoke, Bristol BS32 9DQ (GB). CHAN, David [GB/US]; 16112 Mays Avenue, Monte Sereno, CA 95030 (US). (74) Agent: LAWRENCE, Richard, Anthony; Hewlett-Packard Limited, Intellectual Property Section, Filton Road, Stoke Gifford, Bristol BS34 8QZ (GB).		(81) Designated States: JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>

(54) Title: PROTECTION OF THE CONFIGURATION OF MODULES IN COMPUTING APPARATUS**(57) Abstract**

A method of protecting from modification computer apparatus comprising a plurality of functional modules by monitoring the configuration of functional modules within the computer apparatus. The method comprises: storing a module configuration of the computer apparatus; and checking the actual module configuration against the stored module configuration, and inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration. Advantageously, the module configuration is stored on a security token, such as a smart card.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Protection of the Configuration of Modules in Computing Apparatus

Technical Field

This invention relates to the protection of configuration of modules in a computing apparatus.

Background Art

Today, most modules (the word "module" is used here to describe essentially any discrete functional element of a computing platform) used in computing apparatus are standardised and freely interchangeable. This is advantageous, in that it lowers both the assembly cost and repair cost for computer apparatus, but has the disadvantage that it is relatively easy for computer apparatus to be reassembled from stolen modules, or to be counterfeited.

Much consideration has been given to the problem of making theft or counterfeiting of computer apparatus less attractive. Various proposals have been made as to how to render stolen apparatus inoperable. One approach is for computer apparatus to be fitted with a security device (such as a dedicated application specific integrated circuit) which can enable or disable function of the computer apparatus. This security device is adapted to receive signals (by means of a secure communications link) from a remote station, and only enables function of the computer apparatus if a desired signal is detected during an appropriate validation routine. On theft of the apparatus, the owner notifies the remote station, and the signal necessary to allow the security device to enable function of the computer apparatus is no longer broadcast.

This prior art solution is useful to prevent a thief from using stolen apparatus directly, but is of no assistance in preventing assembly of new (possibly counterfeit) apparatus by the thief from stolen modules - this is a significant practical concern. The more general, and probably more important, problem, is protection of the configuration of modules within a computer apparatus, and the prevention of reuse of stolen modules in a new configuration.

Summary of the Invention

Accordingly, in a first aspect the invention provides a method of protecting from modification computer apparatus comprising a plurality of functional modules by

monitoring the configuration of functional modules within the computer apparatus, the method comprising: storing a module configuration of the computer apparatus; and checking the actual module configuration against the stored module configuration, and inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration.

Use of stored module configurations in this way allows reuse of modules of computer apparatus to be detected and prevented.

Preferably, the stored module configuration is held separately from the computing apparatus. Whether or not stored separately, it is particularly desirable for the stored module configuration to be stored such that it is accessible only by a cryptographic authentication process.

Of particular interest is the case of a host platform which has, directly or indirectly, the facility to verify the existence and functions of the modules in the platform. The present application is particularly relevant to the case of a computer platform which contains verifiable modules and which is adapted to be "trusted" by a user, in the sense that something can be "trusted" if it always behaves in the expected manner for the intended purpose. It is very desirable to prevent computer platforms of this type from being reassembled by an unauthorised party, particularly from stolen modules.

Should trusted platforms of this type become standard, providing the possibility of checking the module configuration of platforms would make theft of computer apparatus that is a part of such a platform much less attractive.

Advantageously, therefore, the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner, and the trusted device is adapted to perform the step of checking the actual module configuration against the stored module configuration.

Preferably, the trusted device is adapted to communicate securely with the stored module configuration. Advantageously, the stored module configuration is held separately from the computer apparatus in a security token - most advantageously a smart card.

In a second aspect, the invention provides computer apparatus adapted for protection against modification, the computer apparatus comprising a plurality of modules, wherein the computer apparatus is adapted to compare a module configuration of the computer apparatus against a stored module configuration.

In a third aspect, the invention provides a security token adapted to hold a stored module configuration of modules in a computer apparatus, and adapted to

provide the stored module configuration to the computer apparatus to allow comparison between an actual module configuration of the computer apparatus and the stored module configuration.

In a fourth aspect, the invention provides a service for storing module configurations of computer apparatus remotely from such computer apparatus, wherein the service provides a stored module configuration to a user authorised to receive it.

In one advantageous approach, the service is invoked by the computer apparatus in a step of checking an actual module configuration against the stored module configuration. The step of checking an actual module configuration against the stored module configuration may involve a security token, and the service is invoked in the event of loss of the security token. The service may also be invoked in order to allow modification to the module configuration of computer apparatus.

In order to protect configuration of modules in a trusted platform, the use in a cooperative arrangement of the trusted device, a portable security token and the group of modules used in the host platform proves to be particularly effective. Typically, the arrangement implements a security control policy to establish a module configuration profile that lists the registered module group, and to authenticate the modules listed with help of the portable security token.

It is particularly desirable to implement mutual/unilateral authentication and privilege restriction. In particular, preferred embodiments utilise a novel method of binding the identity of the portable security token with varieties of the modules.

In one preferred arrangement, such computer apparatus comprises: memory means storing the instructions of a secure process and an authentication process; processing means arranged to control the operation of the computing apparatus including by executing the secure process and the authentication process as required; user interface means arranged to receive user input and return to the user information generated by the processing means in response to the user input; interface between the computing apparatus and a portable security token means for receiving the token and communicating with the token, the token comprising a body supporting: a token interface for communicating with the interface means; a token processor; and token memory storing token data including information for identifying the token; wherein the processing means is arranged to receive the identity information from the portable token, authenticate the token using the authentication process and, if the token is successfully authenticated, permit a user to interact with the secure process via the user interface means for the purpose of establishing and

modifying a module configuration profile comprising a list of registered modules; type, model, identity and other related information of each module included in the list; and if it is not possible to authenticate the portable token, suspending the interaction between the computing apparatus and the user.

In another preferred arrangement, there is provided a method of controlling computing apparatus to authenticate a module listed in the module configuration profile via an interface between a trusted component and the module means for the trusted component receiving the module and communicating with the module, the module comprising a body supporting: a module interface for communicating with the interface means; module memory storing memory data including information for identifying the module; and the trusted component comprising a body supporting: a component interface for communicating with the above interface means; a component processor; and component memory storing component data including information for identifying the component, wherein the processing means is arranged to receive the identity information from the modules, authenticate the module using the authentication process and, if the module is successfully authenticated, permit a user to interact with the secure process via the user interface means, and if it is not possible to authenticate the module, suspending the interaction between the computing apparatus and the user.

Brief Description of the Drawings

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, of which:

Figure 1 is a diagram that illustrates a system capable of implementing embodiments of the present invention;

Figure 2 is a diagram which illustrates a motherboard including a trusted device arranged to communicate with a smart card via a smart card reader and with a group of modules;

Figure 3 is a diagram that illustrates the trusted device in more detail;

Figure 4 is a flow diagram which illustrates the steps involved in acquiring an integrity metric of the computing apparatus;

Figure 5 is a flow diagram which illustrates the steps involved in establishing communications between a trusted computing platform and a remote platform including the trusted platform verifying its integrity;

Figure 6 is a flow diagram which illustrates the steps involved in verification of a trusted computing platform by a potential user of that platform by means of a smart card;

Figure 7 is a diagram that illustrates the operational parts of a smart card adapted for use in embodiments of the present invention;

Figure 8 is a flow diagram that illustrates one example for a host platform to authenticate a module with cryptographic identity;

Figure 9 is a flow diagram that illustrates one example for the host platform to authenticate a module with serial number identity;

Figure 10 is a flow diagram that illustrates one example for the host platform to verify the authorisation of a module without distinguishable identity.

Description of the Preferred Embodiment

The present invention is generally relevant to the prevention of reconfiguration of computer apparatus by an unauthorised user. The embodiments described relate to a particularly preferred case, in which the computer apparatus is a "trusted" platform (one that is designed always to behave in an expected manner for an intended purpose).

For the purpose of preventing unauthorised reconfiguration, each computer apparatus has a module configuration profile. The profile includes a list of registered modules. The attributes of each module listed in the profile may include type, model, manufacturer, statistically unique identity if there exists one, usage privilege and other related information.

This module configuration profile can be held in a number of different ways, as will be discussed further below. However, in particularly preferred embodiments of the invention the module configuration profile is held on a security token such as smart card. Such a smart card is here termed an MCA (Module Configuration Authority) smart card, or "MCA smart card". The MCA smart card is adapted to communicate in a secure manner with a trusted device within the trusted platform. The trusted device and the MCA smart card (or other security token) could be a secure pair with a trusted relationship based on strong authentication between each other.

By transferring the module configuration profile to the trusted device, the security token introduces each module listed in the profile to the trusted device, which is then able to authenticate those modules. It is strongly desirable that both the

security token and the trusted device have the function of tamper-resistant storage to store the module configuration profile.

After a reset of the trusted computing platform, the trusted device checks whether every module present in the platform is listed in the module configuration profile. For the sake of simplicity of description, only three types of modules are considered in any detail herein:

- A module which has a cryptographic identity, that is, one for which the process of authentication requires at least one private key for some cryptographic functions, such as signature and/or decryption. This module can be authenticated by the trusted device without further direct interaction with the MCA smart card. Examples of this type of module include a smart card with cryptographic functions, a cryptographic coprocessor, and a hard disk drive with security functions.
- A module which has a built-in serial number as an identity, which is at least statistically unique and is stored inside the module in a tamper-resistant fashion. This module may or may not be able to be authenticated by the trusted device without direct interaction with the MCA smart card. Examples of this type of module include a smart card with secure storage function, a network card, and an Intel Pentium III processor.
- A module which has no distinguishable identity. Such a module is freely interchangeable and the authorisation of the module can be ensured with direct interaction with the MCA smart card. For example, when the trusted device meets a module without a distinguishable identity, the device will ask for presentation of the MCA smart card to confirm a valid authorisation of the module.

The elements and the operation of a trusted platform (containing a trusted device used in the operations indicated above) will now be described. After that, a smart card appropriate for use as an MCA smart card (in conjunction with a trusted platform as here described) will also be described. The process of authorisation for each of the three types of module described above will then be described also.

The embodiment of a trusted platform here described has as its central feature the incorporation into a computing platform of a physical trusted device whose function is to bind the identity of the platform to reliably measured data that provides an integrity metric of the platform. The identity and the integrity metric are

compared with expected values provided by a trusted party (TP) that is prepared to vouch for the trustworthiness of the platform. If there is a match, the implication is that at least part of the platform is operating correctly, depending on the scope of the integrity metric.

A user verifies the correct operation of the platform before exchanging other data with the platform. A user does this by requesting the trusted device to provide its identity and an integrity metric. (Optionally the trusted device will refuse to provide evidence of identity if it itself was unable to verify correct operation of the platform.) The user receives the proof of identity and the identity metric, and compares them against values which it believes to be true. Those proper values are provided by the TP or another entity that is trusted by the user. If data reported by the trusted device is the same as that provided by the TP, the user trusts the platform. This is because the user trusts the entity. The entity trusts the platform because it has previously validated the identity and determined the proper integrity metric of the platform.

Once a user has established trusted operation of the platform, he exchanges other data with the platform. For a local user, the exchange might be by interacting with some software application running on the platform. For a remote user, the exchange might involve a secure transaction. In either case, the data exchanged is 'signed' by the trusted device. The user can then have greater confidence that data is being exchanged with a platform whose behaviour can be trusted.

The trusted device uses cryptographic processes but does not necessarily provide an external interface to those cryptographic processes. Also, a most desirable implementation would be to make the trusted device tamperproof, to protect secrets by making them inaccessible to other platform functions and provide an environment that is substantially immune to unauthorised modification. Since tamper-proofing is impossible, the best approximation is a trusted device that is tamper-resistant, or tamper-detecting. The trusted device, therefore, preferably consists of one physical component that is tamper-resistant.

Techniques relevant to tamper-resistance are well known to those skilled in the art of security. These techniques include methods for resisting tampering (such as appropriate encapsulation of the trusted device), methods for detecting tampering (such as detection of out of specification voltages, X-rays, or loss of physical integrity in the trusted device casing), and methods for eliminating data when tampering is detected. Further discussion of appropriate techniques can be found at <http://www.cl.cam.ac.uk/~mgk25/tamper.html>. It will be appreciated that, although tamper-proofing is a most desirable feature of the present invention, it does not enter

into the normal operation of the invention and, as such, is beyond the scope of the present invention and will not be described in any detail herein.

The trusted device is preferably a physical one because it must be difficult to forge. It is most preferably tamper-resistant because it must be hard to counterfeit. It typically has an engine capable of using cryptographic processes because it is required to prove identity, both locally and at a distance, and it contains at least one method of measuring some integrity metric of the platform with which it is associated.

A trusted platform 10 is illustrated in the diagram in Figure 1. The platform 10 includes the standard features of a keyboard 14, mouse 16 and visual display unit (VDU) 18, which provide the physical 'user interface' of the platform. This embodiment of a trusted platform also contains a smart card reader 12 - a smart card reader is not an essential element of all trusted platforms, but is employed in various preferred embodiments described below. Along side the smart card reader 12, there is illustrated a smart card 19 to allow trusted user interaction with the trusted platform as shall be described further below. In the platform 10, there are a plurality of modules 15: these are other functional elements of the trusted platform of essentially any kind appropriate to that platform (the functional significance of such elements is not relevant to the present invention and will not be discussed further herein).

As illustrated in Figure 2, the motherboard 20 of the trusted computing platform 10 includes (among other standard components) a main processor 21, main memory 22, a trusted device 24, a data bus 26 and respective control lines 27 and lines 28, BIOS memory 29 containing the BIOS program for the platform 10 and an Input/Output (IO) device 23, which controls interaction between the components of the motherboard and the smart card reader 12, the keyboard 14, the mouse 16 and the VDU 18. The main memory 22 is typically random access memory (RAM). In operation, the platform 10 loads the operating system, for example Windows NT™, into RAM from hard disk (not shown). Additionally, in operation, the platform 10 loads the processes or applications that may be executed by the platform 10 into RAM from hard disk (not shown).

Typically, in a personal computer the BIOS program is located in a special reserved memory area, the upper 64K of the first megabyte of the system memory (addresses F000h to FFFFh), and the main processor is arranged to look at this memory location first, in accordance with an industry wide standard.

The significant difference between the platform and a conventional platform is that, after reset, the main processor is initially controlled by the trusted device, which then hands control over to the platform-specific BIOS program, which in turn

initialises all input/output devices as normal. After the BIOS program has executed, control is handed over as normal by the BIOS program to an operating system program, such as Windows NT (TM), which is typically loaded into main memory 22 from a hard disk drive (not shown).

Clearly, this change from the normal procedure requires a modification to the implementation of the industry standard, whereby the main processor 21 is directed to address the trusted device 24 to receive its first instructions. This change may be made simply by hard-coding a different address into the main processor 21. Alternatively, the trusted device 24 may be assigned the standard BIOS program address, in which case there is no need to modify the main processor configuration.

It is highly desirable for the BIOS boot block to be contained within the trusted device 24. This prevents subversion of the obtaining of the integrity metric (which could otherwise occur if rogue software processes are present) and prevents rogue software processes creating a situation in which the BIOS (even if correct) fails to build the proper environment for the operating system.

Although, in the preferred embodiment to be described, the trusted device 24 is a single, discrete component, it is envisaged that the functions of the trusted device 24 may alternatively be split into multiple devices on the motherboard, or even integrated into one or more of the existing standard devices of the platform. For example, it is feasible to integrate one or more of the functions of the trusted device into the main processor itself, provided that the functions and their communications cannot be subverted. This, however, would probably require separate leads on the processor for sole use by the trusted functions. Additionally or alternatively, although in the present embodiment the trusted device is a hardware device that is adapted for integration into the motherboard 20, it is anticipated that a trusted device may be implemented as a 'removable' device, such as a dongle, which could be attached to a platform when required. Whether the trusted device is integrated or removable is a matter of design choice. However, where the trusted device is separable, a mechanism for providing a logical binding between the trusted device and the platform should be present.

The trusted device 24 comprises a number of blocks, as illustrated in Figure 3. After system reset, the trusted device 24 performs a secure boot process to ensure that the operating system of the platform 10 (including the system clock and the display on the monitor) is running properly and in a secure manner. During the secure boot process, the trusted device 24 acquires an integrity metric of the computing platform 10. The trusted device 24 can also perform secure data transfer

and, for example, authentication between it and a smart card via encryption/decryption and signature/verification. The trusted device 24 can also securely enforce various security control policies, such as locking of the user interface.

Specifically, the trusted device comprises: a controller 30 programmed to control the overall operation of the trusted device 24, and interact with the other functions on the trusted device 24 and with the other devices on the motherboard 20; a measurement function 31 for acquiring the integrity metric from the platform 10; a cryptographic function 32 for signing, encrypting or decrypting specified data; an authentication function 33 for authenticating a smart card; and interface circuitry 34 having appropriate ports (36, 37 & 38) for connecting the trusted device 24 respectively to the data bus 26, control lines 27 and address lines 28 of the motherboard 20. Each of the blocks in the trusted device 24 has access (typically via the controller 30) to appropriate volatile memory areas 4 and/or non-volatile memory areas 3 of the trusted device 24. Additionally, the trusted device 24 is designed, in a known manner, to be tamper resistant.

For reasons of performance, the trusted device 24 may be implemented as an application specific integrated circuit (ASIC). However, for flexibility, the trusted device 24 is preferably an appropriately programmed micro-controller. Both ASICs and micro-controllers are well known in the art of microelectronics and will not be considered herein in any further detail.

One item of data stored in the non-volatile memory 3 of the trusted device 24 is a certificate 350. The certificate 350 contains at least a public key 351 of the trusted device 24 and an authenticated value 352 of the platform integrity metric measured by a trusted party (TP). The certificate 350 is signed by the TP using the TP's private key prior to it being stored in the trusted device 24. In later communications sessions, a user of the platform 10 can verify the integrity of the platform 10 by comparing the acquired integrity metric with the authentic integrity metric 352. If there is a match, the user can be confident that the platform 10 has not been subverted. Knowledge of the TP's generally-available public key enables simple verification of the certificate 350. The non-volatile memory 35 also contains an identity (ID) label 353. The ID label 353 is a conventional ID label, for example a serial number, that is unique within some context. The ID label 353 is generally used for indexing and labelling of data relevant to the trusted device 24, but is insufficient in itself to prove the identity of the platform 10 under trusted conditions.

The trusted device 24 is equipped with at least one method of reliably measuring or acquiring the integrity metric of the computing platform 10 with which it is associated. In the present embodiment, the integrity metric is acquired by the measurement function 31 by generating a digest of the BIOS instructions in the BIOS memory. Such an acquired integrity metric, if verified as described above, gives a potential user of the platform 10 a high level of confidence that the platform 10 has not been subverted at a hardware, or BIOS program, level. Other known processes, for example virus checkers, will typically be in place to check that the operating system and application program code has not been subverted.

The measurement function 31 has access to: non-volatile memory 3 for storing a hash program 354 and a private key 355 of the trusted device 24, and volatile memory 4 for storing acquired integrity metric in the form of a digest 361. In appropriate embodiments, the volatile memory 4 may also be used to store the public keys and associated ID labels 360a-360n of one or more authentic smart cards 19s that can be used to gain access to the platform 10.

In one preferred implementation, as well as the digest, the integrity metric includes a Boolean value, which is stored in volatile memory 4 by the measurement function 31, for reasons that will become apparent.

A preferred process for acquiring an integrity metric will now be described with reference to Figure 4.

In step 500, at switch-on, the measurement function 31 monitors the activity of the main processor 21 on the data, control and address lines (26, 27 & 28) to determine whether the trusted device 24 is the first memory accessed. Under conventional operation, a main processor would first be directed to the BIOS memory first in order to execute the BIOS program. However, in accordance with the present embodiment, the main processor 21 is directed to the trusted device 24, which acts as a memory. In step 505, if the trusted device 24 is the first memory accessed, in step 510, the measurement function 31 writes to volatile memory 3 a Boolean value which indicates that the trusted device 24 was the first memory accessed. Otherwise, in step 515, the measurement function writes a Boolean value which indicates that the trusted device 24 was not the first memory accessed.

In the event the trusted device 24 is not the first accessed, there is of course a chance that the trusted device 24 will not be accessed at all. This would be the case, for example, if the main processor 21 were manipulated to run the BIOS program first. Under these circumstances, the platform would operate, but would be unable to verify its integrity on demand, since the integrity metric would not be

available. Further, if the trusted device 24 were accessed after the BIOS program had been accessed, the Boolean value would clearly indicate lack of integrity of the platform.

In step 520, when (or if) accessed as a memory by the main processor 21, the main processor 21 reads the stored native hash instructions 354 from the measurement function 31 in step 525. The hash instructions 354 are passed for processing by the main processor 21 over the data bus 26. In step 530, main processor 21 executes the hash instructions 354 and uses them, in step 535, to compute a digest of the BIOS memory 29, by reading the contents of the BIOS memory 29 and processing those contents according to the hash program. In step 540, the main processor 21 writes the computed digest 361 to the appropriate non-volatile memory location 4 in the trusted device 24. The measurement function 31, in step 545, then calls the BIOS program in the BIOS memory 29, and execution continues in a conventional manner.

Clearly, there are a number of different ways in which the integrity metric may be calculated, depending upon the scope of the trust required. The measurement of the BIOS program's integrity provides a fundamental check on the integrity of a platform's underlying processing environment. The integrity metric should be of such a form that it will enable reasoning about the validity of the boot process - the value of the integrity metric can be used to verify whether the platform booted using the correct BIOS. Optionally, individual functional blocks within the BIOS could have their own digest values, with an ensemble BIOS digest being a digest of these individual digests. This enables a policy to state which parts of BIOS operation are critical for an intended purpose, and which are irrelevant (in which case the individual digests must be stored in such a manner that validity of operation under the policy can be established).

Other integrity checks could involve establishing that various other devices, components or apparatus attached to the platform are present and in correct working order. In one example, the BIOS programs associated with a SCSI controller could be verified to ensure communications with peripheral equipment could be trusted. In another example, the integrity of other devices, for example memory devices or co-processors, on the platform could be verified by enacting fixed challenge/response interactions to ensure consistent results - this checking of the configuration of the platform is the domain of the present invention, and is discussed further below with reference to Figures 8 to 10. Where the trusted device 24 is a separable component, some such form of interaction is desirable to provide an appropriate logical binding

between the trusted device 14 and the platform. Also, although in the present embodiment the trusted device 24 utilises the data bus as its main means of communication with other parts of the platform, it would be feasible, although not so convenient, to provide alternative communications paths, such as hard-wired paths or optical paths. Further, although in the present embodiment the trusted device 24 instructs the main processor 21 to calculate the integrity metric in other embodiments, the trusted device itself is arranged to measure one or more integrity metrics.

Preferably, the BIOS boot process includes mechanisms to verify the integrity of the boot process itself. Such mechanisms are already known from, for example, Intel's draft "Wired for Management baseline specification v 2.0 - BOOT Integrity Service", and involve calculating digests of software or firmware before loading that software or firmware. Such a computed digest is compared with a value stored in a certificate provided by a trusted entity, whose public key is known to the BIOS. The software/firmware is then loaded only if the computed value matches the expected value from the certificate, and the certificate has been proven valid by use of the trusted entity's public key. Otherwise, an appropriate exception handling routine is invoked.

Optionally, after receiving the computed BIOS digest, the trusted device 24 may inspect the proper value of the BIOS digest in the certificate and not pass control to the BIOS if the computed digest does not match the proper value. Additionally, or alternatively, the trusted device 24 may inspect the Boolean value and not pass control back to the BIOS if the trusted device 24 was not the first memory accessed. In either of these cases, an appropriate exception handling routine may be invoked.

Figure 5 illustrates the flow of actions by a TP, the trusted device 24 incorporated into a platform, and a user (of a remote platform) who wants to verify the integrity of the trusted platform. It will be appreciated that substantially the same steps as are depicted in Figure 5 are involved when the user is a local user. In either case, the user would typically rely on some form of software application to enact the verification. It would be possible to run the software application on the remote platform or the trusted platform. However, there is a chance that, even on the remote platform, the software application could be subverted in some way. Therefore, it is anticipated that, for a high level of integrity, the software application would reside on a smart card of the user, who would insert the smart card into an appropriate reader for the purposes of verification. Figure 5 illustrates the flow of actions for the general

case - a more specific flow of actions for verification by a user smart card will be described with reference to Figure 6 further below.

At the first instance, a TP, which vouches for trusted platforms, will inspect the type of the platform to decide whether to vouch for it or not. This will be a matter of policy. If all is well, in step 600, the TP measures the value of integrity metric of the platform. Then, the TP generates a certificate, in step 605, for the platform. The certificate is generated by the TP by appending the trusted device's public key, and optionally its ID label, to the measured integrity metric, and signing the string with the TP's private key.

The trusted device 24 can subsequently prove its identity by using its private key to process some input data received from the user and produce output data, such that the input/output pair is statistically impossible to produce without knowledge of the private key. Hence, knowledge of the private key forms the basis of identity in this case. Clearly, it would be feasible to use symmetric encryption to form the basis of identity. However, the disadvantage of using symmetric encryption is that the user would need to share his secret with the trusted device. Further, as a result of the need to share the secret with the user, while symmetric encryption would in principle be sufficient to prove identity to the user, it would be insufficient to prove identity to a third party, who could not be entirely sure the verification originated from the trusted device or the user.

In step 610, the trusted device 24 is initialised by writing the certificate 350 into the appropriate non-volatile memory locations 3 of the trusted device 24. This is done, preferably, by secure communication with the trusted device 24 after it is installed in the motherboard 20. The method of writing the certificate to the trusted device 24 is analogous to the method used to initialise smart cards by writing private keys thereto. The secure communications is supported by a 'master key', known only to the TP, that is written to the trusted device (or smart card) during manufacture, and used to enable the writing of data to the trusted device 24; writing of data to the trusted device 24 without knowledge of the master key is not possible.

At some later point during operation of the platform, for example when it is switched on or reset, in step 615, the trusted device 24 acquires and stores the integrity metric 361 of the platform.

When a user wishes to communicate with the platform, in step 620, he creates a nonce, such as a random number, and, in step 625, challenges the trusted device 24 (the operating system of the platform, or an appropriate software application, is arranged to recognise the challenge and pass it to the trusted device

24, typically via a BIOS-type call, in an appropriate fashion). The nonce is used to protect the user from deception caused by replay of old but genuine signatures (called a 'replay attack') by untrustworthy platforms. The process of providing a nonce and verifying the response is an example of the well-known 'challenge/response' process.

In step 630, the trusted device 24 receives the challenge and creates an appropriate response. This may be a digest of the measured integrity metric and the nonce, and optionally its ID label. Then, in step 635, the trusted device 24 signs the digest, using its private key, and returns the signed digest, accompanied by the certificate 350, to the user.

In step 640, the user receives the challenge response and verifies the certificate using the well known public key of the TP. The user then, in step 650, extracts the trusted device's 24 public key from the certificate and uses it to decrypt the signed digest from the challenge response. Then, in step 660, the user verifies the nonce inside the challenge response. Next, in step 670, the user compares the computed integrity metric, which it extracts from the challenge response, with the proper platform integrity metric, which it extracts from the certificate. If any of the foregoing verification steps fails, in steps 645, 655, 665 or 675, the whole process ends in step 680 with no further communications taking place.

Assuming all is well, in steps 685 and 690, the user and the trusted platform use other protocols to set up secure communications for other data, where the data from the platform is preferably signed by the trusted device 24.

Further refinements of this verification process are possible. It is desirable that the challenger becomes aware, through the challenge, both of the value of the platform integrity metric and also of the method by which it was obtained. Both these pieces of information are desirable to allow the challenger to make a proper decision about the integrity of the platform. The challenger also has many different options available - it may accept that the integrity metric is recognised as valid in the trusted device 24, or may alternatively only accept that the platform has the relevant level of integrity if the value of the integrity metric is equal to a value held by the challenger (or may hold there to be different levels of trust in these two cases).

The techniques of signing, using certificates, and challenge/response, and using them to prove identity, are well known to those skilled in the art of security and therefore need not be described in any more detail herein.

As indicated above, Figure 6 shows the flow of actions in an example of verification of platform integrity by a user interacting with the trusted platform with a

smart card 19. As will be described, the process conveniently implements a challenge/response routine. There exist many available challenge/response mechanisms. The implementation of an authentication protocol used in the present embodiment is mutual (or 3-step) authentication, as described in ISO/IEC 9798-3, "Information technology – Security techniques – Entity authentication mechanisms; Part 3; Entity authentication using a public key algorithm", International Organization for Standardization, November 1993. Of course, there is no reason why other authentication procedures cannot be used, for example 2-step or 4-step, as also described in this reference.

Initially, the user inserts their smart card 19 into the smart card reader 12 of the platform in step 700.

Beforehand, a platform configured for use by users of in this way will typically be operating under the control of its standard operating system and executing the authentication process, which waits for a user to insert their smart card 19. Apart from the smart card reader 12 being active in this way, such a platform is typically rendered inaccessible to users by 'locking' the user interface (i.e. the screen, keyboard and mouse). This will however not be the case in all embodiments of the invention.

When the smart card 19 is inserted into the smart card reader 12, the trusted device 24 is triggered to attempt mutual authentication in step by generating and transmitting a nonce A to the smart card 19 in step 705. A nonce, such as a random number, is used to protect the originator from deception caused by replay of old but genuine responses (called a 'replay attack') by untrustworthy third parties.

In response, in step 710, the smart card 19 generates and returns a response comprising the concatenation of: the plain text of the nonce A, a new nonce B generated by the smart card 19, an ID of the trusted device 24 and some redundancy; the signature of the plain text, generated by signing the plain text with the private key of the smart card 19; and a certificate containing the ID and the public key of the smart card 19.

The trusted device 24 authenticates the response by using the public key in the certificate to verify the signature of the plain text in step 715. If the response is not authentic, the process ends in step 720. If the response is authentic, in step 725 the trusted device 24 generates and sends a further response including the concatenation of: the plain text of the nonce A, the nonce B, an ID of the smart card 19 and the acquired integrity metric; the signature of the plain text, generated by signing the plain text using the private key of the trusted device 24; and the certificate

comprising the public key of the trusted device 24 and the authentic integrity metric, both signed by the private key of the TP.

The smart card 19 authenticates this response by using the public key of the TP and comparing the acquired integrity metric with the authentic integrity metric, where a match indicates successful verification, in step 730. If the further response is not authentic, the process ends in step 735.

If the procedure is successful, both the trusted device 24 has authenticated the logon card 19 and the smart card 19 has verified the integrity of the trusted platform and, in step 740, the authentication process executes the secure process for the user.

In certain types of interaction, the authentication process can end at this point. However, if a session is to be continued between the user and the trusted platform, it is desirable to ensure that the user remains authenticated to the platform.

Where continued authentication is required, the authentication process sets an interval timer in step 745. Thereafter, using appropriate operating system interrupt routines, the authentication process services the interval timer periodically to detect when the timer meets or exceeds a pre-determined timeout period in step 750.

Clearly, the authentication process and the interval timer run in parallel with the secure process. When the timeout period is met or exceeded, the authentication process triggers the trusted device 24 to re-authenticate the smart card 19, by transmitting a challenge for the smart card 19 to identify itself in step 760. The smart card 19 returns a certificate including its ID and its public key in step 765. In step 770, if there is no response (for example, as a result of the smart card 19 having been removed) or the certificate is no longer valid for some reason (for example, the smart card has been replaced with a different smart card), the session is terminated by the trusted device 24 in step 775. Otherwise, in step 770, the process from step 745 repeats by resetting the interval timer.

Additionally, or alternatively, in some embodiments it may be required that the user profile is encrypted and signed to protect privacy and integrity. If so, a secure data transfer protocol may be needed between the trusted device 24 and the smart card 19. There exist many available mechanisms for transferring secure credentials between two entities. A possible implementation, which may be used in the present embodiment, is secure key transport mechanisms from ISO/IEC DIS 11770-3, "Information technology – Security techniques – Key management - Part 3: Mechanisms using asymmetric techniques", International Organization for Standardization, March 1997.

Modifications of this verification process using other well-known challenge and response techniques can easily be achieved by the skilled person. Similarly, alternative verification processes can be used by parties interacting with the platform in a different manner (that is, other than as a user equipped with a smart card).

A smart card suitable for use as an MCA card in accordance with a preferred embodiment of the invention will now be described. Such a smart card may be essentially an authorised smart card 19 as described above, and may thus interact with the trusted platform 10 and trusted device 24 as described above with reference to Figure 6.

A processing part 40 of the smart card 19 is illustrated in Figure 7. As shown, the smart card processing part 40 has the standard smart card features of a processor 41, a memory 42 and interface contacts 43. The processor 41 is programmed for simple challenge/response operations involving authentication of the smart card 19 and verification of the platform 10, as is described above (with reference to Figure 6) and will be described below (with reference to Figures 8 to 10). The memory 42 contains the smart card private key 420, the smart card public key 428, a module configuration profile 421, the public key 422 of the trusted platform and an identity 427. The module configuration profile 421 lists the registered modules 15 AC1-ACn usable by the computer apparatus (typically, the computer apparatus will be the trusted platform itself - however, the computer apparatus whose configuration is to be verified may be apparatus somehow associated with the trusted platform rather than the trusted platform itself - for example, a peripheral to the trusted platform, or a device on the same local area network as the trusted platform), and the individual security policy 424 for the computer apparatus. For each module 15, the module configuration profile includes respective identification information 423, the trust structure 425 between the modules (if one exists) and, optionally, the type or make 426 of the module.

In the module configuration profile 421, each module 15 entry AC1-ACn includes associated identification information 423, which varies depending upon the type of module (cryptographic identity, serial number identity, or no unique identity)

The 'security policy' 424 dictates the options that a user has on the platform 10 while verifying a module 15. For example, the user interface may be locked or unlocked while a module 15 is authenticated, depending on the function of the module 15. Additionally, or alternatively, certain files or executable programs on the platform 10 may be made accessible or inaccessible, depending on the level of trust

for a particular module 15. Moreover, if authentication for a module 15 fails, the user interface may be locked, in which event it cannot be accessed by the user at all, or the user interface may be left unlocked, but in a state such that the functions associated with this unauthorised module are not available for the user.

A 'trust structure' 425 defines whether a module 15 can itself 'introduce' further modules 15 into the system without first requiring authorisation from the MCA smart card 19. In the embodiments described in detail herein, the only defined trust structure is between the MCA smart card 19 and the modules 15 that can be introduced to the platform 10 by the MCA smart card 19. Allowing specified modules 15 to introduce further modules would preferably require such a module 15 to have an equivalent of a module configuration profile listing the or each module that it is able to introduce. To prevent misuse, it is desirable for such a module must be removable, and to be stored apart from the host platform.

As indicated above, authentication between an MCA smart card 19 and the platform can be achieved by the process set out in Figure 6 above. It will typically not be necessary for the reauthorisation loop to be used, as module configuration authorisation will typically not need to be carried out repeatedly throughout a user session.

When authentication is achieved, the trusted device 24 then interrogates all the modules 15 in the computer apparatus to be validated (typically, but not necessarily, the trusted platform 10 itself). Authentication of different types of module is discussed further below. The trusted device 24 thus obtains an actual module configuration profile - this is compared with the stored module configuration profile on the MCA smart card 19. The result of this comparison is treated in accordance with the security policy 424, with results ranging from uninhibited use of the computer apparatus by the user in the case of a total match, to inhibited or no use of the computer apparatus in the case of a less than total match.

In one possible arrangement, the trusted device 24 and the MCA smart card 19 may be a specific pair, whereby a user is not able to use one smart card to authorise more than one platform and/or a platform cannot be authorised by using more than one smart card. Clearly, this is not the only possibility. Alternatively, one smart card may be adapted to function for more than one platform and/or one platform can be authorised by using more than one smart card.

It may be desirable to ensure that there is a recovery service for MCA smart cards. If such a recovery service exists, if one smart card is lost, the owner of the corresponding platform can ask the recovery service to change the authority

relationship from the lost MCA smart card to another MCA smart card. Clearly, the recovery service must exercise great care in making this change, and a high level of trust between the recovery service and each trusted platform concerned is required.

Processes for authenticating the different module types (cryptographic identity, serial number identity, and no self-identity) will now be described.

A preferred process for authenticating a cryptographic identity module 15 by a platform 10 will be described with reference to the flow diagram in Figure 8. As will be described, the process conveniently implements a challenge/response routine. Again, there exist many available challenge/response mechanisms. The implementation of an authentication protocol used in the present embodiment is unilateral authentication with 2-pass, as described in ISO/IEC 9798-3. Of course, there is no reason why other authentication procedures cannot be used, for example 1-pass, as also described in ISO/IEC 9798-3.

Initially in step 800, the trusted device 24 retrieves a module configuration profile listing the identity information of the module, which may be a certificate of a public key corresponding with the module's private key. It is assumed that the trusted device 24 can verify the validation of the certificate of the module's public key. It then challenges the module by sending a nonce in step 805. After receiving the nonce, in step 810, the MCA smart card 19 generates and returns a response comprising the concatenation of: the plain text of the nonce, the ID 353 of the trusted device 24 and some redundancy; the signature of the plain text, generated by signing the plain text with the private key of the MCA smart card 19; and a certificate containing the ID and the public key of the MCA smart card 19.

The trusted device 24 authenticates the response by using the public key in the certificate to verify the signature of the plain text in step 815. If the response is not authentic, the process ends in step 820. If the response is authentic, in step 830, the authentication process executes some secure processes between the trusted device 24 and the MCA smart card 19.

A preferred process for authenticating a serial number identity module 15 by a platform 10 will be described with reference to the flow diagram in Figure 9. The trusted device 24 needs to check if the serial number and other related information of the module match with the data about this module listed in the module configuration profile. If the trusted device 24 is unable to obtain the serial number of a module in a sufficiently secure manner, then it will not be advisable to follow this approach (the

approach shown in Figure 10, in which the MCA smart card 19 plays a positive role, is required).

Initially, the trusted device 24 retrieves a module configuration profile listing the identity information of the module in step 900, then it requests the serial number of the module in step 905. The module 15 returns the response with its serial number in step 910. The trusted device 24 compares this serial number with the data recorded in the module configuration profile in step 915. If it matches, the authentication passes and the following secure process will carry on in step 930; otherwise, the authentication is failed in step 920.

A preferred process for verifying authorisation of a module without self-identity 15 by a platform 10 will be described with reference to the flow diagram in Figure 10. The authorisation of usage of the module can be ensured with on-line help of the MCA smart card.

Initially, the trusted device 24 retrieves a module configuration profile listing the identity information of the module in step 1000. When the trusted device 24 meets a module 15 without a distinguishable identity, the trusted device 24 will ask for presentation of the MCA smart card 19 to confirm a valid authorisation of the module. To do so, the trusted device first displays a message to request an MCA smart card 19 in step 1025, and second locks the user interface in step 1030. The user inserts the MCA smart card 19 in step 1033. Authentication between the trusted device 24 and the MCA smart card 19 can choose either unilateral authentication or mutual authentication as shown above. In Figure 8, we use a unilateral authentication with 2-pass, as described in ISO/IEC 9798-3. The trusted device 24 challenges the MCA smart card 19 in step 1040, and the MCA smart card 19 responds in step 845. The trusted device 24 authenticates the response in step 1050. If the response is not authentic, the process aborts in step 1055. If the response is authentic, the trusted device accepts the corresponding module, and the following secure process will carry on in step 1060.

If, during the process of authentication of modules, a module is not successfully authenticated, an appropriate measure may be taken in accordance with the security policy 424, such as locking of the user interface. If the authentication procedure fails for any other reason, such as removal of the MCA smart card, the user interface may be temporarily locked - if the user inserts the MCA smart card 19, a new round of authentication is performed between the MCA smart card 19 and the platform 10. Upon successful verification, the user interface will be unlocked.

It is clear that where a trusted computing platform 10 has an associated MCA smart card 19, the MCA smart card 19 should be kept safely and preferably remotely from the platform 10. It is desirable for the MCA smart card 19 to be provided with appropriate security protection, such as a user password, to ensure that it is only used in an authorised manner.

Although in the embodiment described above, the module configuration is stored in a local smart card, other possibilities of providing module configuration in accordance with the invention are available. The module configuration may be provided by a remote smart card, communicating with the trusted platform by an appropriate communication system (most conveniently, by the Internet, though essentially any other communication networks suitable for carrying the relevant amount of data could be suitable). Appropriate secure communication between the remote smart card and the trusted platform 10 can be established by conventional means (essentially as indicated above for communication between a local smart card 19 and the trusted platform 10), although a greater level of encryption may be required. The module configuration may be held with another form of security token (other than a smart card), either locally or remotely.

A further possibility is for the module configuration information to be held on a remote server. Clearly, there will need to be an appropriate trust relationship between the remote server and the trusted platform, together with an appropriate communication path (typically the Internet) and, preferably, secure communication - otherwise the relationship and interactions between the remote server and the trusted platform may be essentially the same as between the MCA smart card and the trusted platform as described above, and the skilled person. There is thus the possibility of having a module configuration authorisation server holding a large number of module configurations, and providing module configuration authorisation as a service.

A further alternative is to have a remote module configuration authorisation (MCA) server as an addition, rather than an alternative, to an MCA smart card. An owner of a computer apparatus could be offered the alternative of using an MCA smart card, an MCA server, or both (requiring the trusted device to communicate with both the MCA smart card and the MCA server for either proper function or reconfiguration). An advantage of requiring MCA server authorisation for function of the computer apparatus is that if both the computer apparatus and the MCA smart card have been stolen, then the owner can notify the operator of the MCA server and the MCA server will no longer authorise operation of the computer apparatus.

Clearly, it is necessary for there to be a mechanism to allow module configurations to be established and modified. Establishment could take place in an initialisation routine after assembly of the trusted platform 10 (in which, for example, the trusted device 24 in communication with MCA smart card 19 interrogates all modules 15 in the trusted platform 10 to establish their identities and records the results to the MCA smart card 19 in a manner comparable to that in which the initial value of the integrity metric is established and stored). Modification may then be allowed by an appropriate user routine when communication with the MCA smart card 19 is subsequently established - for example, when module configuration changes are detected, the user may be requested to authorise such changes (preferably after invocation of an appropriate security mechanism to establish that the user is authorised, such as a password). Where an MCA server and an MCA smart card 19 both exist, a practical arrangement may be to allow routine validation with the MCA smart card 19 alone but only to allow module configuration changes with the cooperation of the MCA server (the opposite arrangement may also be advantageous in some systems - allowing routine validation with an MCA server but configuration changes only with the MCA smart card 19).

Although the embodiments described above use a trusted platform having a trusted device, this arrangement is highly advantageous rather than essential to operation of the invention. An appropriate mechanism is required for checking the modules in the computer apparatus against a securely held module configuration, and also for inhibiting function of the computer apparatus (in accordance with an appropriate security policy), but these could be achieved by means other than a trusted device as described in the preferred embodiments - for example, by appropriate software in the computer apparatus (although this solution is likely to be less secure than would be the case with use of a trusted device). However, for computer apparatus other than a general purpose computing platform, use of software or another solution (such as a dedicated ASIC) may be a satisfactory solution.

Claims

1. A method of protecting from modification computer apparatus comprising a plurality of functional modules by monitoring the configuration of functional modules within the computer apparatus, the method comprising:

storing a module configuration of the computer apparatus; and

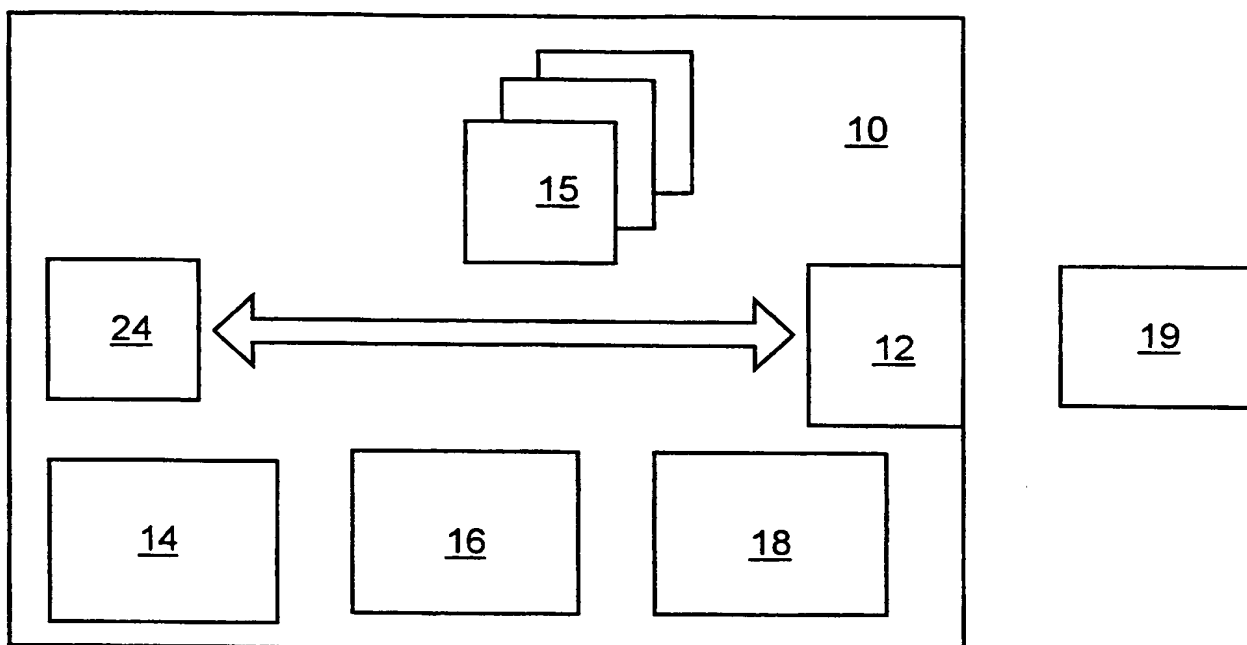
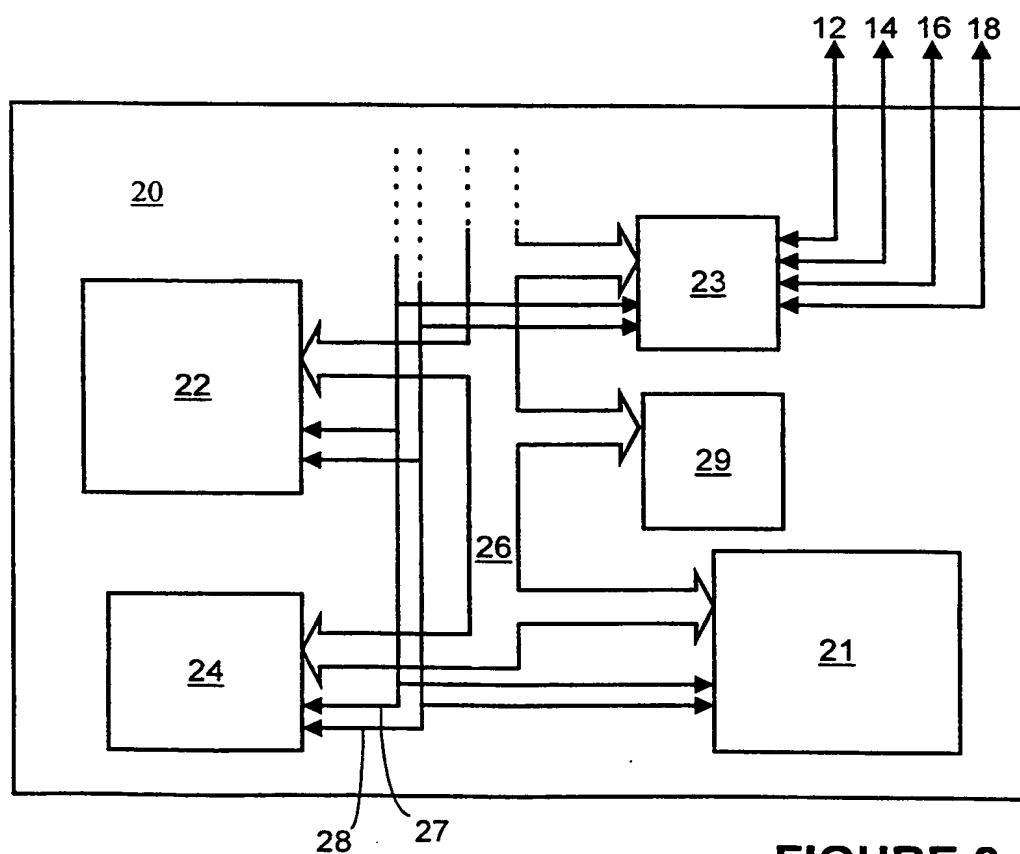
checking the actual module configuration against the stored module configuration, and inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration.
2. A method as claimed in claim 1, wherein the stored module configuration is held separately from the computing apparatus.
3. A method as claimed in claim 1 or claim 2, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process.
4. A method as claimed in any preceding claim, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner, and wherein the trusted device is adapted to perform the step of checking the actual module configuration against the stored module configuration.
5. A method as claimed in claim 4 where dependent on claim 2, wherein the trusted device is adapted to communicate securely with the stored module configuration.
6. A method as claimed in claim 5, wherein the stored module configuration is stored in a security token.
7. A method as claimed in claim 6, wherein the security token is a smart card.

8. A method as claimed in any preceding claim, wherein the step of checking of the actual module configuration comprises a cryptographic identification process for modules with a cryptographic identity.
9. A method as claimed in any preceding claim, wherein a stored module configuration is held by a remote module validation authority.
10. A method as claimed in claim 9, wherein the step of checking the actual module configuration against the stored module configuration involves use of the stored module configuration held by the remote module validation authority.
11. A method as claimed in claim 9 or claim 10 where dependent on claim 6, wherein the remote validation authority provides a service allowing a replacement security token to be provided if a security token is lost or stolen.
12. Computer apparatus adapted for protection against modification, the computer apparatus comprising a plurality of modules, wherein the computer apparatus is adapted to compare a module configuration of the computer apparatus against a stored module configuration.
13. Computer apparatus as claimed in claim 12, wherein the stored module configuration is held separately from the computing apparatus and wherein the computer apparatus is adapted to obtain the stored module configuration by a cryptographic authentication process.
14. Computer apparatus as claimed in claim 12 or claim 13, wherein the computer apparatus further comprises a trusted device adapted to respond to a user in a trusted manner, and wherein the trusted device is adapted to perform the step of checking the actual module configuration against the stored module configuration.
15. A security token adapted to hold a stored module configuration of modules in a computer apparatus, and adapted to provide the stored module configuration to the computer apparatus to allow comparison between an

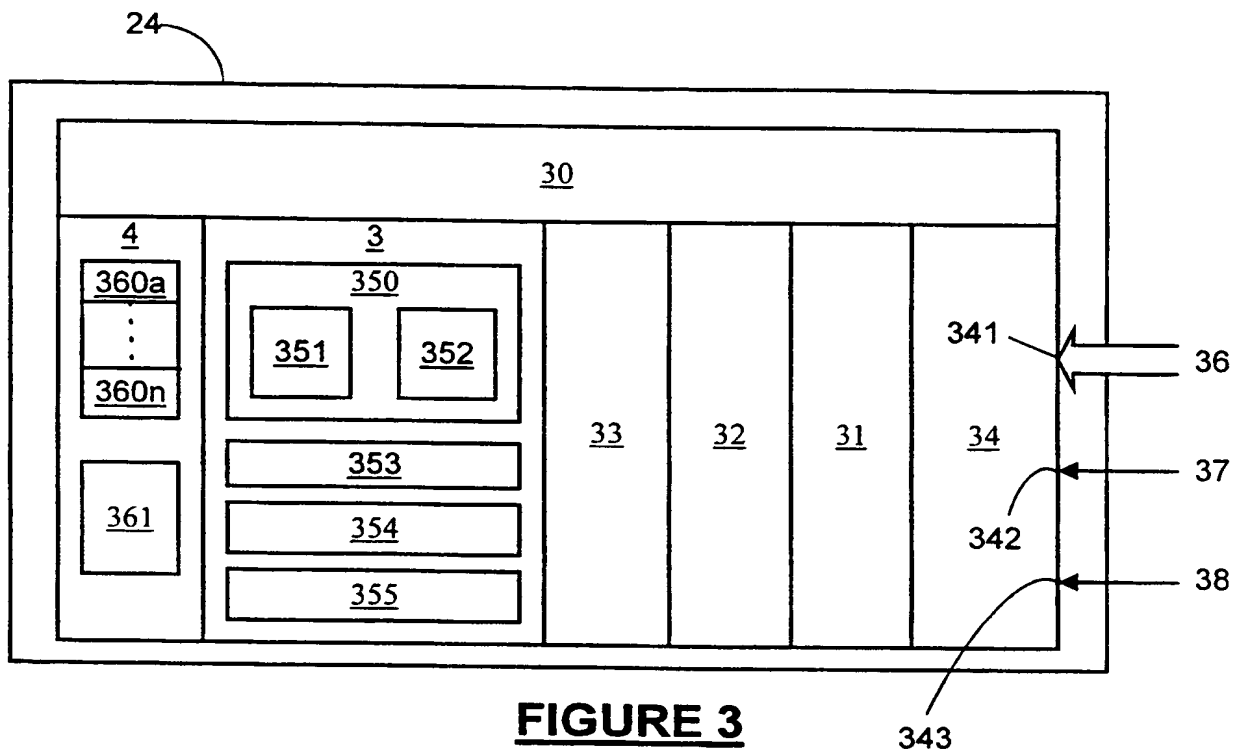
actual module configuration of the computer apparatus and the stored module configuration.

16. A security token as claimed in claim 15, wherein the stored module configuration is held in an encrypted form.
17. A security token as claimed in claim 15 or claim 16, wherein the security token is a smart card.
18. A service for storing module configurations of computer apparatus remotely from such computer apparatus, wherein the service provides a stored module configuration to a user authorised to receive it.
19. A service as claimed in claim 18, wherein the service is invoked by the computer apparatus in a step of checking an actual module configuration against the stored module configuration.
20. A service as claimed in claim 19, wherein the step of checking an actual module configuration against the stored module configuration involves a security token, and the service is invoked in the event of loss of the security token.
21. A service as claimed in claim 18, wherein the service is invoked in order to allow modification to the module configuration of computer apparatus.

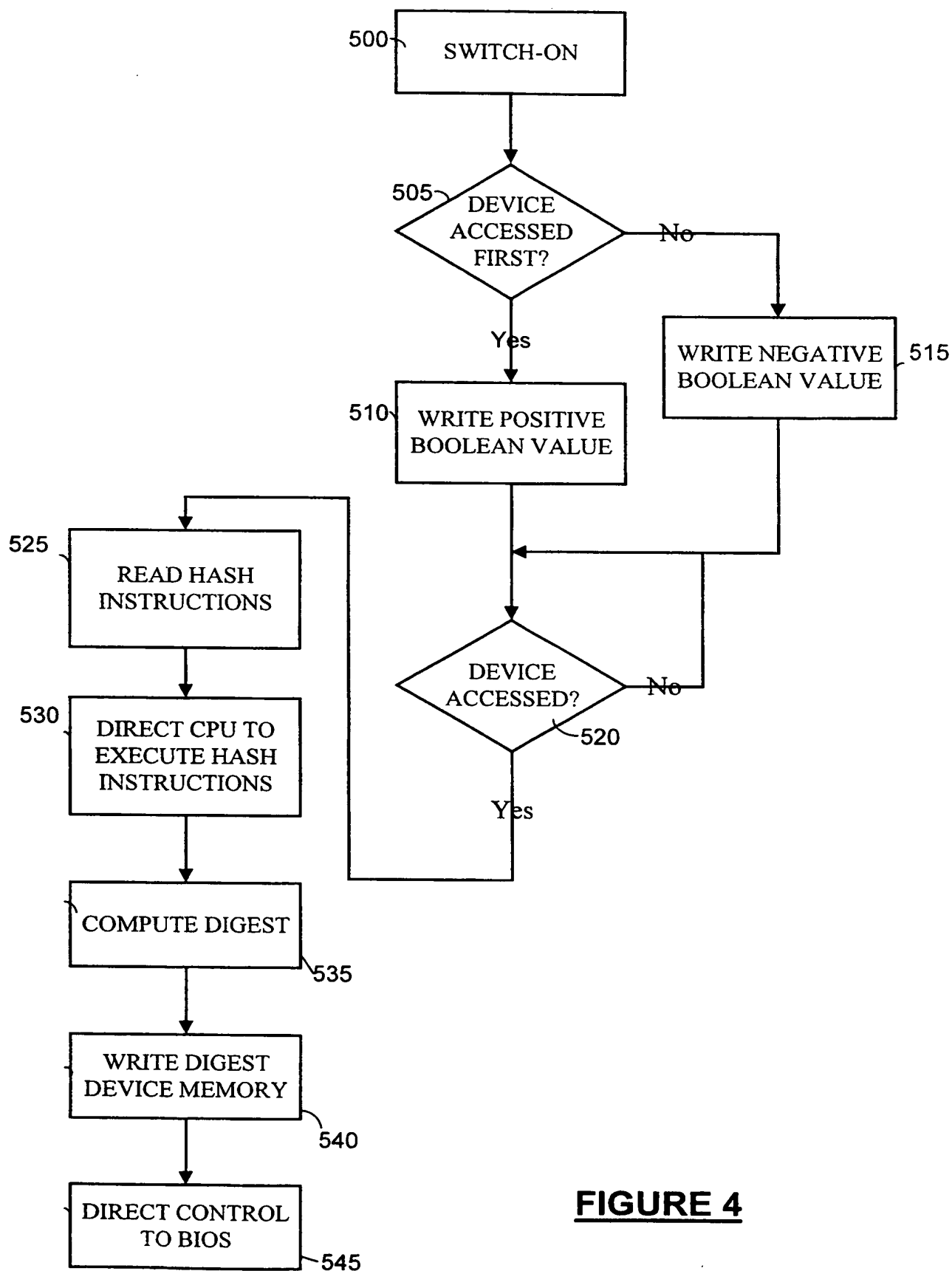
1/9

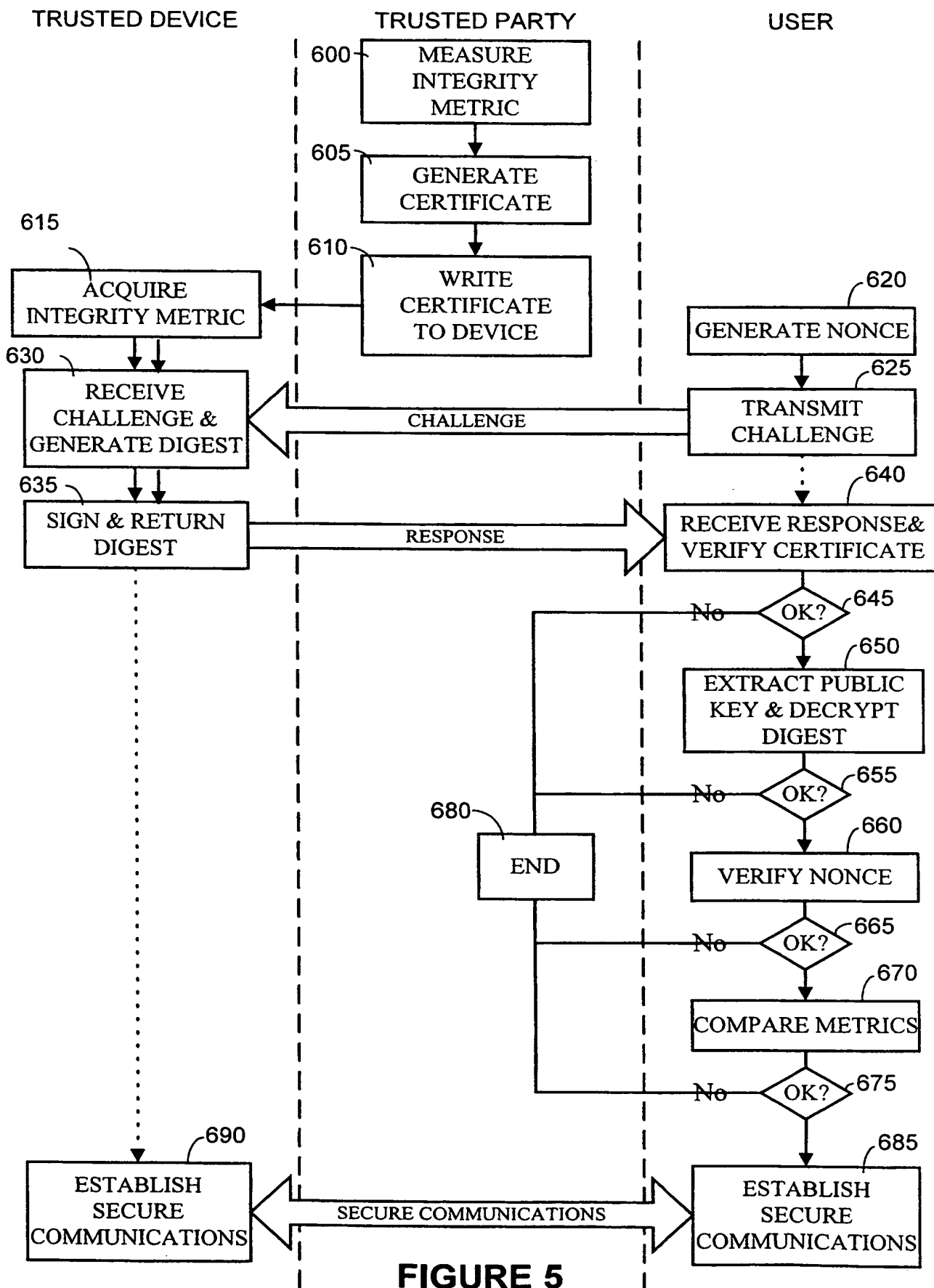
**FIGURE 1****FIGURE 2**

2/9

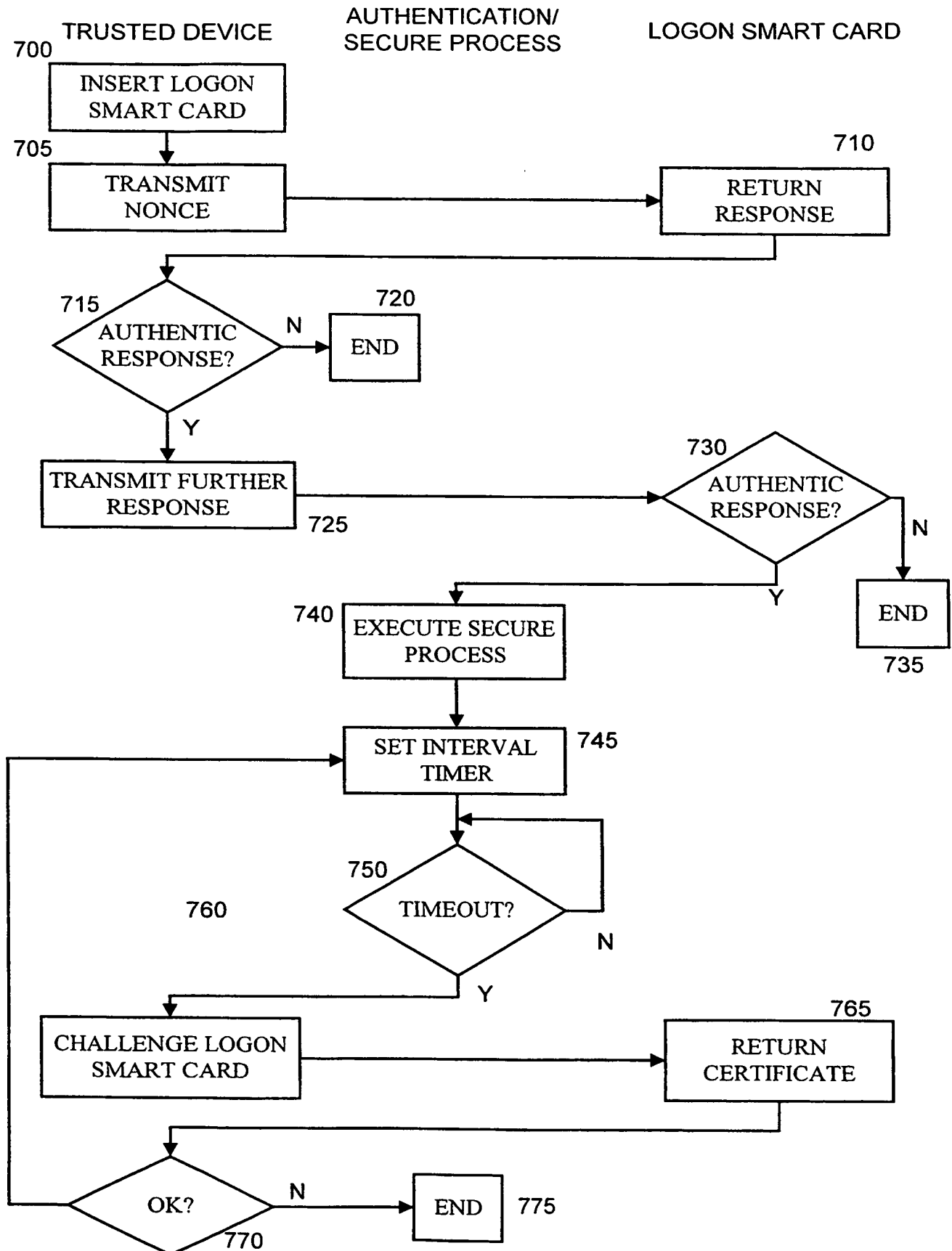


3/9

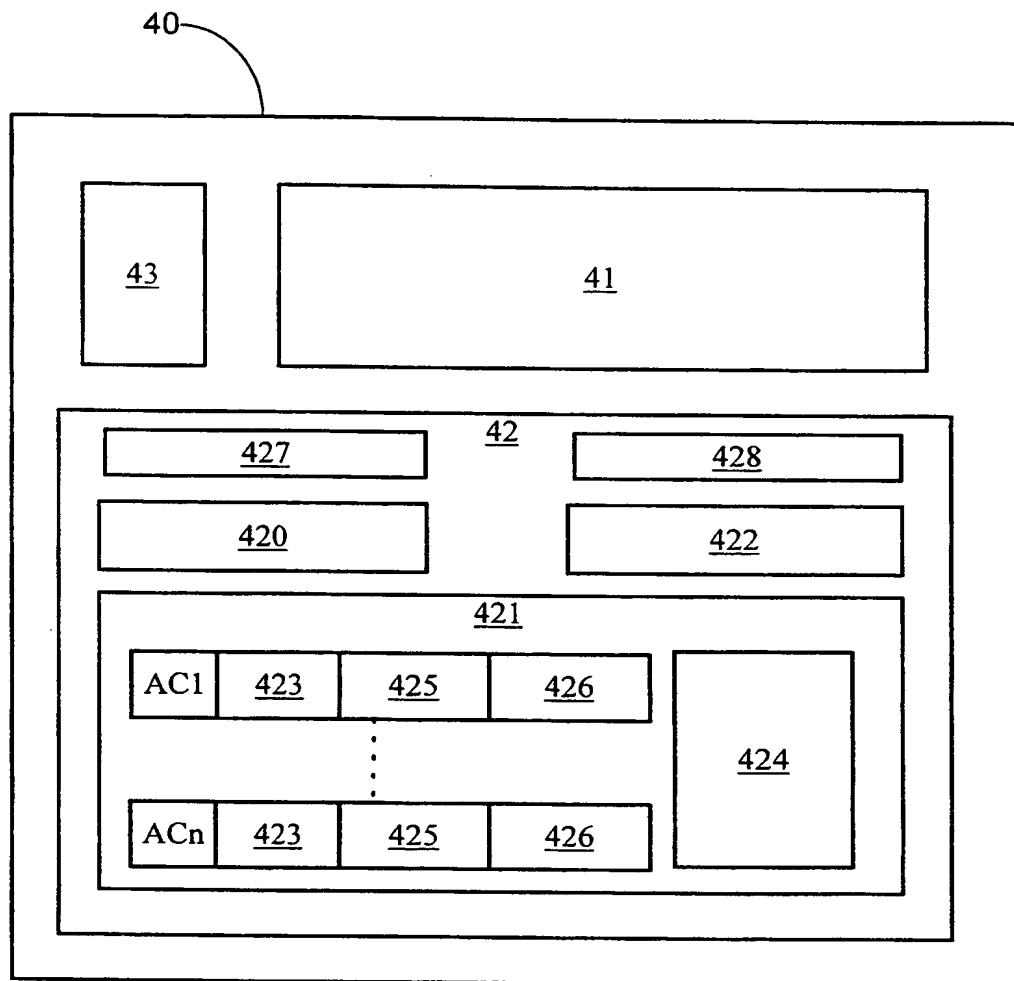
**FIGURE 4**



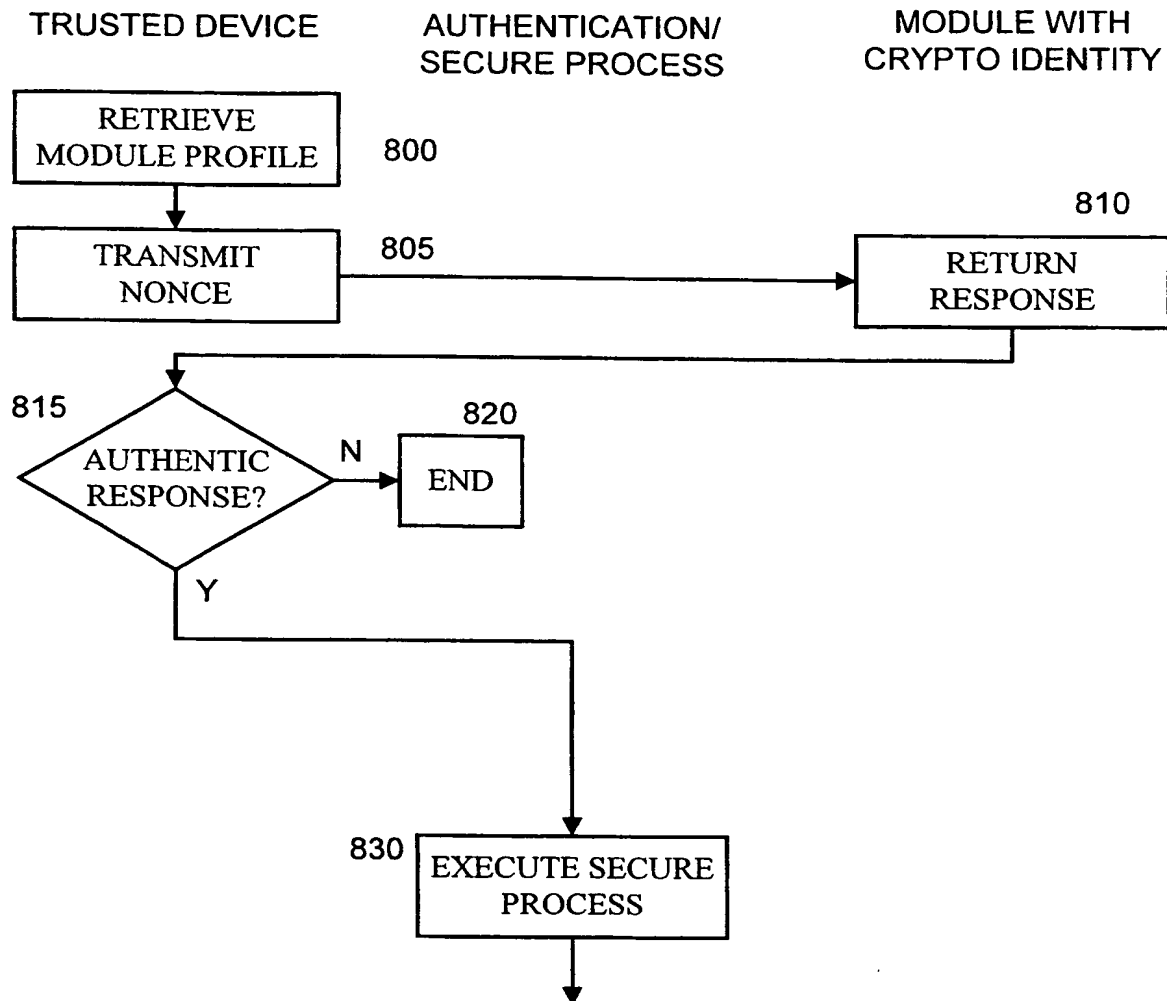
5/9

**FIGURE 6**

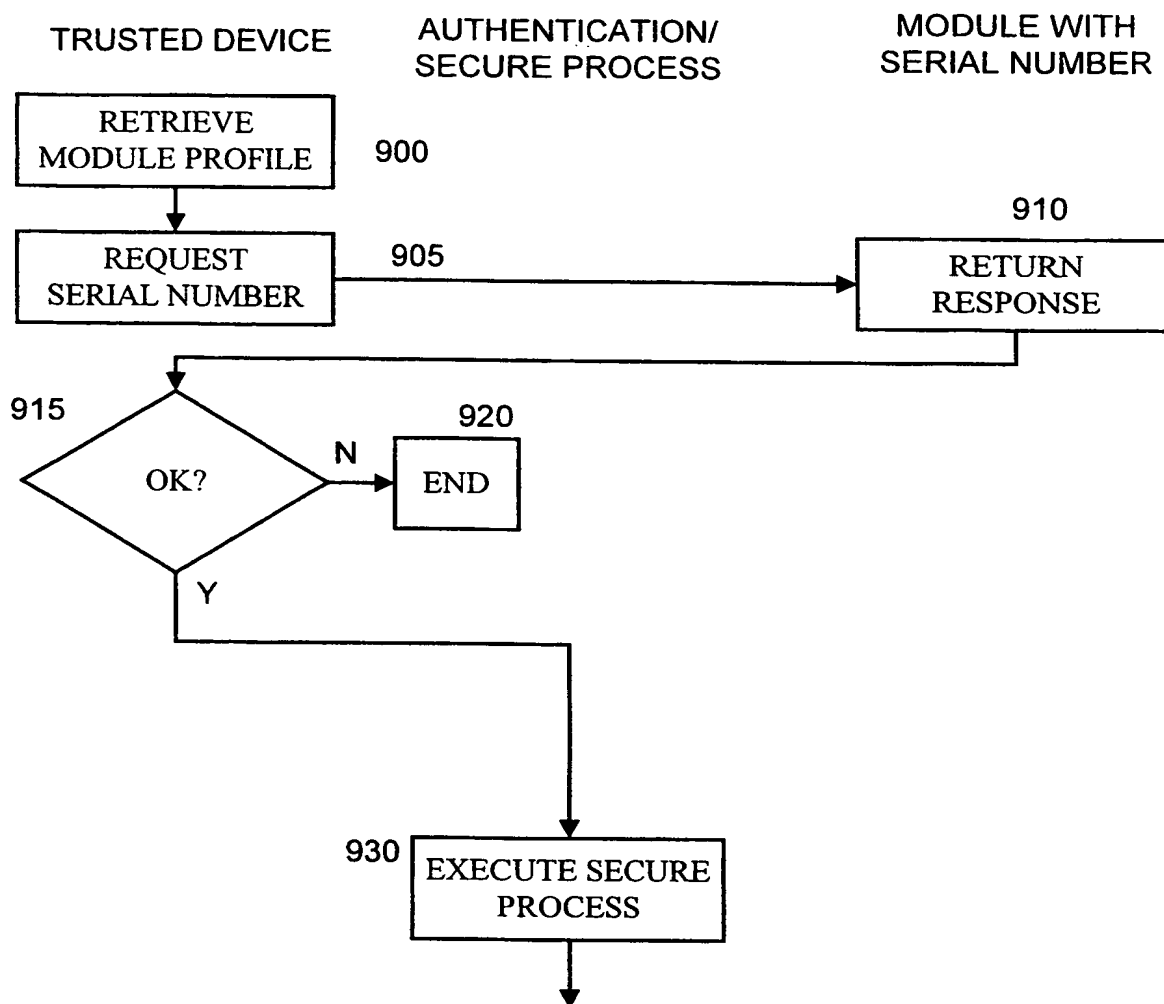
6/9

**FIGURE 7**

7/9

**FIGURE 8**

8/9

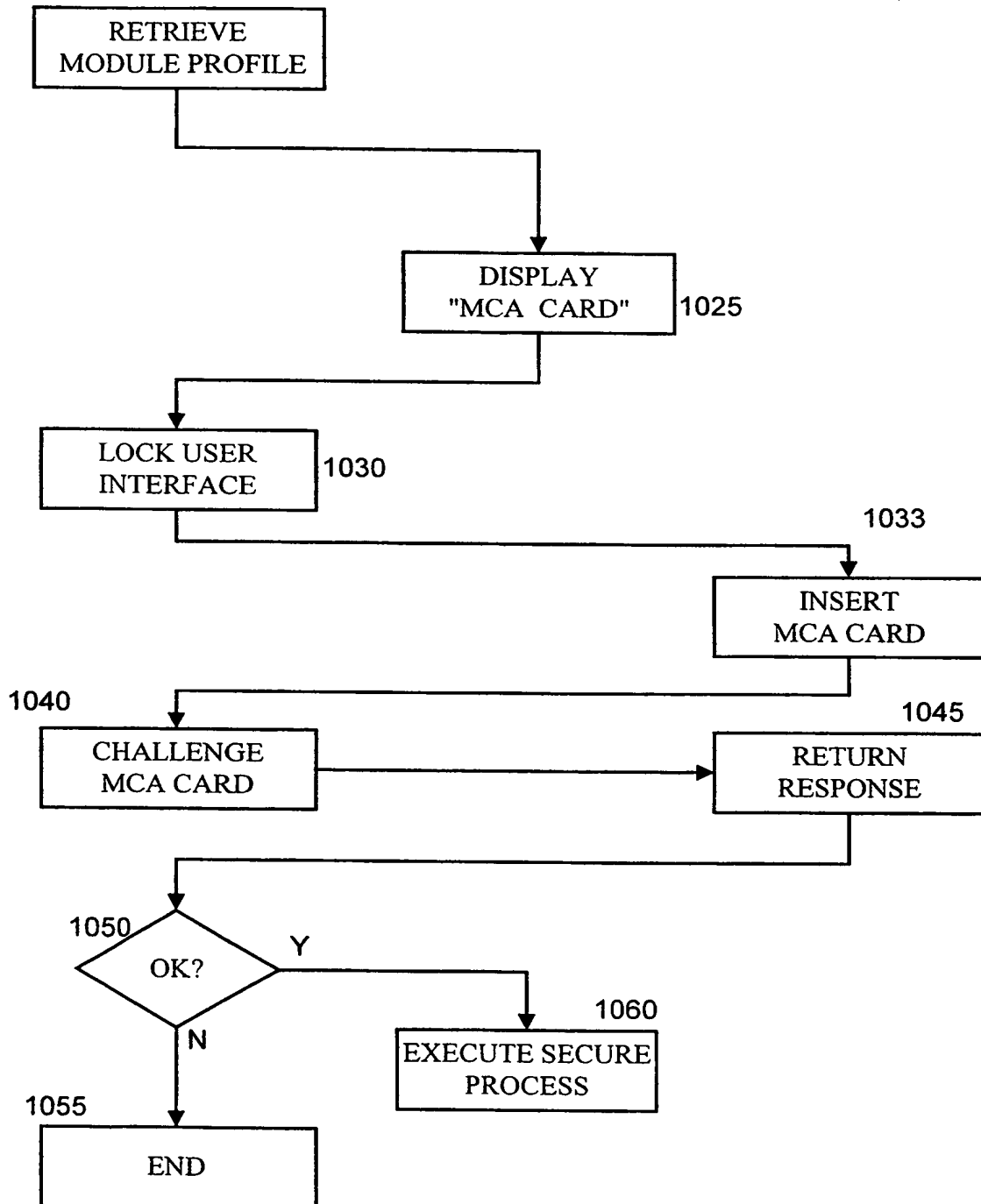
**FIGURE 9**

9/9

TRUSTED DEVICE

AUTHENTICATION/
SECURE PROCESSMODULE WITHOUT
IDENTITY/
MCA SMART CARD

1005

**FIGURE 10**

INTERNATIONAL SEARCH REPORT

Int. Patent Application No

PCT/GB 00/00495

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F11/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 07463 A (PROBST JUERGEN ; IBM (US)) 27 February 1997 (1997-02-27) abstract; figures 1-3 page 5, line 1 -page 8, line 1 page 9, line 19 -page 11, line 8	1-3, 9, 10, 12, 13, 15, 16, 18, 19, 21
Y	-----	4-8, 14, 17
Y	WO 95 24696 A (INTEGRATED TECH AMERICA ; MOONEY DAVID M (US); WOOD DAVID E (US); K) 14 September 1995 (1995-09-14) the whole document ----- -/-	4-8, 14, 17

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

23 June 2000

Date of mailing of the international search report

30/06/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Powell, D

INTERNATIONAL SEARCH REPORT

Inte Application No

PCT/GB 00/00495

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 444 850 A (CHANG STEVE M) 22 August 1995 (1995-08-22) the whole document ----	9, 10, 18, 19, 21
A	EP 0 848 315 A (COMPAQ COMPUTER CORP) 17 June 1998 (1998-06-17) ----	
A	WO 98 15082 A (INTEL CORP) 9 April 1998 (1998-04-09) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/GB 00/00495

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9707463	A	27-02-1997	EP	0787328 A	06-08-1997
			US	5982899 A	09-11-1999
WO 9524696	A	14-09-1995	US	5610981 A	11-03-1997
			AT	175505 T	15-01-1999
			AU	703856 B	01-04-1999
			AU	2092695 A	25-09-1995
			BR	9506968 A	01-06-1999
			CA	2183759 A	14-09-1995
			CN	1146813 A	02-04-1997
			DE	69507129 D	18-02-1999
			DE	69507129 T	05-08-1999
			EP	0748474 A	18-12-1996
			NZ	282954 A	24-11-1997
US 5444850	A	22-08-1995	WO	9613002 A	02-05-1996
			AU	1042895 A	15-05-1996
			JP	10511783 T	10-11-1998
			US	5680547 A	21-10-1997
			EP	0791195 A	27-08-1997
EP 0848315	A	17-06-1998	CN	1195818 A	14-10-1998
			SG	55422 A	21-12-1998
WO 9815082	A	09-04-1998	US	5844986 A	01-12-1998
			AU	4146197 A	24-04-1998
			CN	1231787 A	13-10-1999
			EP	0932953 A	04-08-1999

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

International Application No.

International Filing Date

09/913454

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference
(if desired) (12 characters maximum) 30990085 WO

Box No. I TITLE OF INVENTION

Protection of the Configuration of Modules in Computing Apparatus

Box No. II APPLICANT

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304
US

☐ This person is also inventor.

Telephone No.

Facsimile No.

Teleprinter No.

State (that is, country) of nationality:

US

State (that is, country) of residence:

US

This person is applicant
for the purposes of:

☐ all designated
States

☒ all designated States except
the United States of America

☐ the United States
of America only

☐ the States indicated in
the Supplemental Box
Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)

CHEN, Ligu
1 Harvest Close
Bradley Stoke
Bristol BS32 9DQ
GB

This person is:

☐ applicant only

☒ applicant and inventor

☐ inventor only (If this check-box
is marked, do not fill in below.)

State (that is, country) of nationality:

CN

State (that is, country) of residence:

GB

This person is applicant
for the purposes of:

☐ all designated
States

☐ all designated States except
the United States of America

☒ the United States
of America only

☐ the States indicated in
the Supplemental Box

☒ Further applicants and/or (further) inventors are indicated on a continuation sheet.
Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf
of the applicant(s) before the competent International Authorities as:

☒ agent

☐ common representative

Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)

LAWRENCE, Richard Anthony
Hewlett-Packard Limited
Intellectual Property Section
Filton Road
Stoke Gifford,
Bristol BS34 8QZ
GB

Telephone No.

(0)117-312-8026

Facsimile No.

(0)117-312-8941

Teleprinter No.

☐ Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Continuation of Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)	
<i>If none of the following sub-boxes is used, this sheet should not be included in the request.</i>	
<p>Name and address: <i>(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)</i></p> <p>CHAN, David 16112 Mays Avenue Monte Sereno California CA 95030 US</p>	<p>This person is:</p> <p><input type="checkbox"/> applicant only</p> <p><input checked="" type="checkbox"/> applicant and inventor</p> <p><input type="checkbox"/> inventor only <i>(If this check-box is marked, do not fill in below.)</i></p>
State <i>(that is, country)</i> of nationality: GB	State <i>(that is, country)</i> of residence: US
<p>This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box</p>	
<p>Name and address: <i>(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)</i></p>	<p>This person is:</p> <p><input type="checkbox"/> applicant only</p> <p><input type="checkbox"/> applicant and inventor</p> <p><input type="checkbox"/> inventor only <i>(If this check-box is marked, do not fill in below.)</i></p>
State <i>(that is, country)</i> of nationality:	State <i>(that is, country)</i> of residence:
<p>This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box</p>	
<p>Name and address: <i>(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)</i></p>	<p>This person is:</p> <p><input type="checkbox"/> applicant only</p> <p><input type="checkbox"/> applicant and inventor</p> <p><input type="checkbox"/> inventor only <i>(If this check-box is marked, do not fill in below.)</i></p>
State <i>(that is, country)</i> of nationality:	State <i>(that is, country)</i> of residence:
<p>This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box</p>	
<p>Name and address: <i>(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)</i></p>	<p>This person is:</p> <p><input type="checkbox"/> applicant only</p> <p><input type="checkbox"/> applicant and inventor</p> <p><input type="checkbox"/> inventor only <i>(If this check-box is marked, do not fill in below.)</i></p>
State <i>(that is, country)</i> of nationality:	State <i>(that is, country)</i> of residence:
<p>This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box</p>	
<p>Name and address: <i>(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)</i></p>	<p>This person is:</p> <p><input type="checkbox"/> applicant only</p> <p><input type="checkbox"/> applicant and inventor</p> <p><input type="checkbox"/> inventor only <i>(If this check-box is marked, do not fill in below.)</i></p>
State <i>(that is, country)</i> of nationality:	State <i>(that is, country)</i> of residence:
<p>This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box</p>	
<p><input type="checkbox"/> Further applicants and/or (further) inventors are indicated on another continuation sheet.</p>	

Box No.V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) (mark the applicable check-boxes; at least one must be marked):

Regional Patent

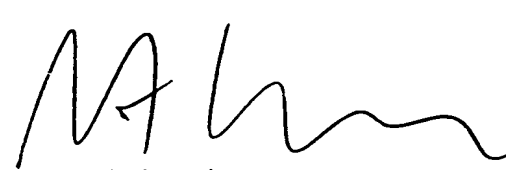
- ☐ **AP ARIPO Patent:** GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- ☐ **EA Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ **EP European Patent:** AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☐ **OA OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (if other kind of protection or treatment desired, specify on dotted line)

National Patent (if other kind of protection or treatment desired, specify on dotted line):

- | | |
|--|--|
| <input type="checkbox"/> AE United Arab Emirates | <input type="checkbox"/> LR Liberia |
| <input type="checkbox"/> AL Albania | <input type="checkbox"/> LS Lesotho |
| <input type="checkbox"/> AM Armenia | <input type="checkbox"/> LT Lithuania |
| <input type="checkbox"/> AT Austria | <input type="checkbox"/> LU Luxembourg |
| <input type="checkbox"/> AU Australia | <input type="checkbox"/> LV Latvia |
| <input type="checkbox"/> AZ Azerbaijan | <input type="checkbox"/> MA Morocco |
| <input type="checkbox"/> BA Bosnia and Herzegovina | <input type="checkbox"/> MD Republic of Moldova |
| <input type="checkbox"/> BB Barbados | <input type="checkbox"/> MG Madagascar |
| <input type="checkbox"/> BG Bulgaria | <input type="checkbox"/> MK The former Yugoslav Republic of Macedonia |
| <input type="checkbox"/> BR Brazil | |
| <input type="checkbox"/> BY Belarus | <input type="checkbox"/> MN Mongolia |
| <input type="checkbox"/> CA Canada | <input type="checkbox"/> MW Malawi |
| <input type="checkbox"/> CH and LI Switzerland and Liechtenstein | <input type="checkbox"/> MX Mexico |
| <input type="checkbox"/> CN China | <input type="checkbox"/> NO Norway |
| <input type="checkbox"/> CR Costa Rica | <input type="checkbox"/> NZ New Zealand |
| <input type="checkbox"/> CU Cuba | <input type="checkbox"/> PL Poland |
| <input type="checkbox"/> CZ Czech Republic | <input type="checkbox"/> PT Portugal |
| <input type="checkbox"/> DE Germany | <input type="checkbox"/> RO Romania |
| <input type="checkbox"/> DK Denmark | <input type="checkbox"/> RU Russian Federation |
| <input type="checkbox"/> DM Dominica | <input type="checkbox"/> SD Sudan |
| <input checked="" type="checkbox"/> EE Estonia | <input type="checkbox"/> SE Sweden |
| <input type="checkbox"/> ES Spain | <input type="checkbox"/> SG Singapore |
| <input type="checkbox"/> FI Finland | <input type="checkbox"/> SI Slovenia |
| <input type="checkbox"/> GB United Kingdom | <input type="checkbox"/> SK Slovakia |
| <input type="checkbox"/> GD Grenada | <input type="checkbox"/> SL Sierra Leone |
| <input type="checkbox"/> GE Georgia | <input type="checkbox"/> TJ Tajikistan |
| <input type="checkbox"/> GH Ghana | <input type="checkbox"/> TM Turkmenistan |
| <input type="checkbox"/> GM Gambia | <input type="checkbox"/> TR Turkey |
| <input type="checkbox"/> HR Croatia | <input type="checkbox"/> TT Trinidad and Tobago |
| <input type="checkbox"/> HU Hungary | <input type="checkbox"/> TZ United Republic of Tanzania |
| <input type="checkbox"/> ID Indonesia | <input type="checkbox"/> UA Ukraine |
| <input type="checkbox"/> IL Israel | <input type="checkbox"/> UG Uganda |
| <input type="checkbox"/> IN India | <input checked="" type="checkbox"/> US United States of America |
| <input type="checkbox"/> IS Iceland | |
| <input checked="" type="checkbox"/> JP Japan | <input type="checkbox"/> UZ Uzbekistan |
| <input type="checkbox"/> KE Kenya | <input type="checkbox"/> VN Viet Nam |
| <input type="checkbox"/> KG Kyrgyzstan | <input type="checkbox"/> YU Yugoslavia |
| <input type="checkbox"/> KP Democratic People's Republic of Korea | <input type="checkbox"/> ZA South Africa |
| | <input type="checkbox"/> ZW Zimbabwe |

Check-boxes reserved for designating States which have become party to the PCT after issuance of this sheet:

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)

Box No. VI PRIORITY CLAIM		<input type="checkbox"/> Further priority claims as indicated in the Supplemental Box.		
Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is:		
		national application: country	regional application: regional Office	international application: receiving Office
item (1) (15.02.99) 15 February 1999	99301100.6		EP	
item (2) (25.09.99) 25 September 1999	9922663.1	GB		
item (3)				
<input type="checkbox"/> The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) (only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office) identified above as item(s):				
<i>* Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.</i>				
Box No. VII INTERNATIONAL SEARCHING AUTHORITY				
Choice of International Searching Authority (ISA) (if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):		Request to use results of earlier search; reference to that search (if an earlier search has been carried out by or requested from the International Searching Authority):		
ISA / EP		Date (day/month/year)	Number	Country (or regional Office)
Box No. VIII CHECK LIST; LANGUAGE OF FILING				
This international application contains the following number of sheets: request : 4 description (excluding sequence listing part) : 23 claims : 3 abstract : 1 drawings : 9 sequence listing part of description : Total number of sheets : 40		This international application is accompanied by the item(s) marked below: 1. <input checked="" type="checkbox"/> fee calculation sheet 2. <input type="checkbox"/> separate signed power of attorney 3. <input checked="" type="checkbox"/> copy of general power of attorney, reference number, if any: 4. <input type="checkbox"/> statement explaining lack of signature 5. <input checked="" type="checkbox"/> priority document(s) identified in Box No. VI as item(s): 1, 2 6. <input type="checkbox"/> translation of international application into (language): 7. <input type="checkbox"/> separate indications concerning deposited microorganism or other biological material 8. <input type="checkbox"/> nucleotide and/or amino acid sequence listing in computer readable form 9. <input type="checkbox"/> other (specify):		
Figure of the drawings which should accompany the abstract: 7		Language of filing of the international application: English		
Box No. IX SIGNATURE OF APPLICANT OR AGENT				
Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).				
 Richard Anthony Lawrence				

For receiving Office use only	
1. Date of actual receipt of the purported international application: 3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application: 4. Date of timely receipt of the required corrections under PCT Article 11(2): 5. International Searching Authority (if two or more are competent): ISA /	2. Drawings: <input type="checkbox"/> received: <input type="checkbox"/> not received: 6. <input type="checkbox"/> Transmittal of search copy delayed until search fee is paid.

For International Bureau use only
Date of receipt of the record copy by the International Bureau:

PCT

FEE CALCULATION SHEET Annex to the Request

For receiving Office use only

International application No.

Date stamp of the receiving Office

Applicant's or agent's
file reference 30990085 WO

Applicant

HEWLETT-PACKARD COMPANY

CALCULATION OF PRESCRIBED FEES

1. TRANSMITTAL FEE £55 T

2. SEARCH FEE £838 S

International search to be carried out by EP

(If two or more International Searching Authorities are competent in relation to the international application, indicate the name of the Authority which is chosen to carry out the international search.)

3. INTERNATIONAL FEE

Basic Fee

The international application contains £264 sheets.

first 30 sheets £264 b1

10 x £6 = £60 b2

remaining sheets additional amount

Add amounts entered at b1 and b2 and enter total at B £324 B

Designation Fees

The international application contains 3 designations.

3 x 56 = £168 D

number of designation fees amount of designation fee payable (maximum 8)

Add amounts entered at B and D and enter total at I £492 I

(Applicants from certain States are entitled to a reduction of 75% of the international fee. Where the applicant is (or all applicants are) so entitled, the total to be entered at I is 25% of the sum of the amounts entered at B and D.)

4. FEE FOR PRIORITY DOCUMENT (if applicable) P

5. TOTAL FEES PAYABLE £1185

Add amounts entered at T, S, I and P, and enter total in the TOTAL box TOTAL

☐ The designation fees are not paid at this time.

MODE OF PAYMENT

☒ authorization to charge
deposit account (see below)

☐ bank draft

☐ coupons

☐ cheque

☐ cash

☐ other (specify):

☐ postal money order

☐ revenue stamps

DEPOSIT ACCOUNT AUTHORIZATION (this mode of payment may not be available at all receiving Offices)

The RO/ GB ☒ is hereby authorized to charge the total fees indicated above to my deposit account.

☒ (this check-box may be marked only if the conditions for deposit accounts of the receiving Office so permit) is hereby authorized to charge any deficiency or credit any overpayment in the total fees indicated above to my deposit account.

☐ is hereby authorized to charge the fee for preparation and transmittal of the priority document to the International Bureau of WIPO to my deposit account.

D01463

Deposit Account No.

Date (day/month/year) 15/02/00

Signature

The demand must be filed directly with the competent International Preliminary Examining Authority or, if more Authorities are competent, with the one chosen by the applicant. The full name or two-letter code of that Authority may be indicated by the applicant on the line below:

IPEA/ EP

09/913454

PCT

CHAPTER II

DEMAND

under Article 31 of the Patent Cooperation Treaty:

The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

For International Preliminary Examining Authority use only

Identification of IPEA		Date of receipt of DEMAND
Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION		Applicant's or agent's file reference 30990085 WO
International application No. PCT/GB 00/00495	International filing date (day/month/year) 15 February 2000 (15/02/00)	(Earliest) Priority date (day/month/year) 15 February 1999 (15/02/99)
Title of invention Protection of the configuration of Modules in Computing Apparatus		
Box No. II APPLICANT(S)		
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.) Hewlett-Packard Company 3000 Hanover Street Palo Alto CA 94304 USA		Telephone No.: Facsimile No.: Teleprinter No.:
State (that is, country) of nationality: US	State (that is, country) of residence: US	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.) CHEN, Liquan 1 Harvest Close Bradley Stoke Bristol BS32 9DQ GB		
State (that is, country) of nationality: CN	State (that is, country) of residence: GB	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.) CHAN, David 16112 Mays Avenue Monte Sereno CA 95030 US		
State (that is, country) of nationality: GB	State (that is, country) of residence: US	
<input type="checkbox"/> Further applicants are indicated on a continuation sheet.		

Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCEThe following person is ☒ agent ☐ common representativeand ☒ has been appointed earlier and represents the applicant(s) also for international preliminary examination.☐ is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.☐ is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*LAWRENCE, Richard Anthony
Hewlett-Packard Limited
Intellectual Property Section
Filton Road
Stoke Gifford
Bristol BS34 8QZ
GB

Telephone No.:

+44-117-312-8295

Facsimile No.:

+44-117-312-8941

Teleprinter No.:

☐ Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.**Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION****Statement concerning amendments:***

1. The applicant wishes the international preliminary examination to start on the basis of:

☒ the international application as originally filed

the description

☐ as originally filed☐ as amended under Article 34

the claims

☐ as originally filed☐ as amended under Article 19 (together with any accompanying statement)☐ as amended under Article 34

the drawings

☐ as originally filed☐ as amended under Article 342. ☐ The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.3. ☐ The applicant wishes the start of the international preliminary examination to be postponed until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). *(This check-box may be marked only where the time limit under Article 19 has not yet expired.)*

* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examination: English☒ which is the language in which the international application was filed.☐ which is the language of a translation furnished for the purposes of international search.☐ which is the language of publication of the international application.☐ which is the language of the translation (to be) furnished for the purposes of international preliminary examination.**Box No. V ELECTION OF STATES**The applicant hereby elects all eligible States *(that is, all States which have been designated and which are bound by Chapter II of the PCT)*

excluding the following States which the applicant wishes not to elect:

Box No. VI CHECKLIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:

- | | | |
|--|---|--------|
| 1. translation of international application | : | sheets |
| 2. amendments under Article 34 | : | sheets |
| 3. copy (or, where required, translation) of amendments under Article 19 | : | sheets |
| 4. copy (or, where required, translation) of statement under Article 19 | : | sheets |
| 5. letter | : | sheets |
| 6. other (<i>specify</i>) | : | sheets |

For International Preliminary Examining Authority use only

received not received

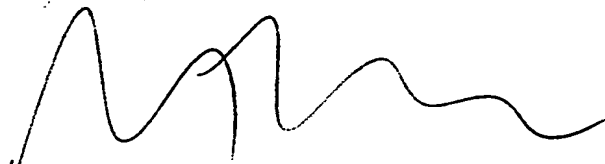
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

The demand is also accompanied by the item(s) marked below:

- | | |
|--|---|
| 1. <input checked="" type="checkbox"/> fee calculation sheet | 4. <input type="checkbox"/> statement explaining lack of signature |
| 2. <input type="checkbox"/> separate signed power of attorney | 5. <input type="checkbox"/> nucleotide and or amino acid sequence listing in computer readable form |
| 3. <input type="checkbox"/> copy of general power of attorney; reference number, if any: | 6. <input type="checkbox"/> other (<i>specify</i>): |

Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).


Richard Anthony Lawrence

For International Preliminary Examining Authority use only

1. Date of actual receipt of DEMAND:

2. Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):

3. ☐ The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply. ☐ The applicant has been informed accordingly.

4. ☐ The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.

5. ☐ Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only



Demand received from IPEA on:

PCT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 30990085 WO		FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/GB00/00495	International filing date (<i>day/month/year</i>) 15/02/2000	Priority date (<i>day/month/year</i>) 15/02/1999	
International Patent Classification (IPC) or national classification and IPC G06F1/00			
Applicant HEWLETT-PACKARD COMPANY et al.			
<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of 9 sheets, including this cover sheet.</p> <p><input type="checkbox"/> This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of sheets.</p>			
<p>3. This report contains indications relating to the following items:</p> <ul style="list-style-type: none"> I <input checked="" type="checkbox"/> Basis of the report II <input type="checkbox"/> Priority III <input checked="" type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV <input type="checkbox"/> Lack of unity of invention V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI <input type="checkbox"/> Certain documents cited VII <input checked="" type="checkbox"/> Certain defects in the international application VIII <input checked="" type="checkbox"/> Certain observations on the international application 			
Date of submission of the demand 15/09/2000		Date of completion of this report 20.06.2001	
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465		Authorized officer Harms, C Telephone No. +49 89 2399 7476 	

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB00/00495

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, pages:

1-23 as originally filed

Claims, No.:

1-21 as originally filed

Drawings, sheets:

1-9 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB00/00495

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 18-21.

because:

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 18-21 are so unclear that no meaningful opinion could be formed (*specify*):
see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)

Yes: Claims

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB00/00495

	No:	Claims	1, 6, 12, 15-16
Inventive step (IS)	Yes:	Claims	
	No:	Claims	2-5, 7-11, 13-14, 17
Industrial applicability (IA)	Yes:	Claims	1-17
	No:	Claims	

2. Citations and explanations
see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

SECTION III

- 1 The category of the independent claim 18 is not clear. Therefore no further examination of this and its dependent claims 19-21 is possible at this stage.

Possibly claim 18 should refer to a computer program for realising an (Internet) service. However, a claim of this kind should read as "a computer program for realising an (Internet) service comprising code means adapted to perform all the steps of claim 1" or an expression the like. Nevertheless such a claim would lack novelty in view of the analysis under section V given below.

SECTION V

Reference is made to the following document:

D1: WO 97 07463

- 1 Taking account to the following references to D1, the subject-matter of independent claim 1 as understood under section VIII is not new because D1 discloses

a method of protecting from modification a computer apparatus (see "verifying of a configuration of a computer system" top of page 1 and "modification detection" on page 3 line 7) comprising a plurality of functional modules (see "high level components within computer 26" on page 12 lines 5-6 and computer 26 containing modules 29-39 in Fig. 4) by monitoring the configuration of functional modules within the computer apparatus (see "verifying of a configuration of a computer system" top of page 1), the method comprising:

storing a module configuration of the computer apparatus (see page 9 lines 25-32 and Fig. 1); and

checking the actual module configuration against the stored module configuration (see page 11 lines 23-25 and step 23 of Fig. 3), and inhibiting function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration (see "stop the booting procedure" on page 11 lines 2-3 and step 25 of Fig. 3)

- 2 Independent claim 12 discloses the apparatus corresponding to the method of claim

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB00/00495

1. Thus claim 12 is not new.
- 3 Independent claim 15 discloses the storage device corresponding to the method of claim 1 and to the apparatus of claim 12 (see also "disk 38" on page 14 line 16 and Fig. 4). Hence claim 15 is not new.
- 4 The term "security token" used in claim 6 encompasses all forms of (secure) storage. Hence claim 6 is not new.
- 5 The storage of sensible data on a smart card such as put forward in claims 7 and 17 is a matter of a normal design procedure. Hence claims 7 and 17 are not inventive.
- 6 Dependent claim 8 refers to the "challenge/response" being well-known in the art (see also application page 14 lines 27-28). Thus claim 8 is not inventive.
- 7 The feature of claim 16 is known from D1 page 14 line 16. Thus claim 16 is not new.
- 8 In the dependent claims 2-5, 9-11 and 13-14 minor modifications to the system as defined in the respective head claims are set out, all of which, when not directly deducted from the teachings of the documents cited in the search report, relate to routine measures normally to be expected of the skilled person.
- 9 It is brought to the attention of the Applicant that the scopes of independent claims 12 and 15 are much broader than the scope of claim 1 since several features of claim 1 have been omitted in claims 12 and 15. This should have been considered when filing amended claims in order to overcome the objections under Arts. 33(2) and (3) PCT.

The scopes of the claims could have been brought in correspondence by inserting "specially adapted to the method of claim 1" into claims 12 and 15.

SECTION VII

- 1 "lines 28" on page 8 line 15 should read "address lines 28" in correspondence with page 10 line 3.

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB00/00495

- 2 "main processor" on page 8 line 28 should have been provided by reference sign 21.
"trusted device" on page 8 line 28, on page 9 lines 17, 19, 20, 21 and 33, on page 12 line 30 should have been provided by reference sign 24.
"platform" on page 9 line 19, page 16 lines 29 and 33, page 17 last line should have been provided by reference sign 10.
"non-volatile memory" on page 10 line 22 should have been provided by reference sign 3 and not 35.
"volatile memory" on page 11 line 17 should have been provided by reference sign 4 and not 3.
"trusted device" on page 12 line 25 should have been provided by reference sign 24 and not 14.
"data bus" on page 12 line 26 should have been provided reference number 26.
"digest of the measured integrity metric" on page 14 line 30 should have been provided by reference sign 361.
"private key" on page 12 line 32 should have been provided by reference sign 355.
"public key" on page 12 line 36 should have been provided by reference sign 351.
"certificate" on page 12 line 36 should have been provided by reference sign 350.
"acquired integrity metric" on page 16 lines 19 and 24 should have been provided by reference sign 361.
"authentic integrity metric" on page 16 line 24 should have been provided by reference sign 252.
"module configuration profile" on page 18 line 8 should have been provided by reference sign 421.

SECTION VII

- 1 The term "does not satisfactorily match" used in claim 1 is vague and unclear and leaves the reader in doubt as to the meaning of the technical feature to which it refers, thereby rendering the definition of the subject-matter of said claim unclear (Art. 6 PCT).

One way to overcome the objection would have been to delete "satisfactorily" in claim 1.

- 2 Claim 3 does not meet the requirements of Article 6 PCT in that the matter for which

protection is sought is not clearly defined. The claim attempt to define the subject-matter in terms of the result to be achieved which merely amounts to a statement of the underlying problem. The technical features necessary for achieving this result should be added.

- 3 The terms "contains or is in communication" and "responding to the user in a trusted manner" used in claim 4 have no well-recognised meaning and leave the reader in doubt as to the meaning of the technical features to which they refer, thereby rendering the definition of the subject-matter of said claim unclear (Art. 6 PCT).

The latter term moreover attempts to define the subject-matter in terms of the result to be achieved which merely amounts to a statement of the underlying problem. The technical features necessary for achieving this result should be added (Art. 6 PCT).

Besides the difference between the "computer apparatus containing communication with a trusted device" and "the computer apparatus being in communication with the trusted device" (see lines 1-2 of claim 4) is not clear. Claim 4 therefore also lacks conciseness, Art. 6 PCT.

One way to overcome the objection against the first term would have been to amend claim 4 to "(...) computer apparatus communicates with a trusted device (...)".

- 4 Claim 5 does not meet the requirements of Article 6 PCT in that the matter for which protection is sought is not clearly defined. The term "adapted to communicate securely" attempts to define the subject-matter in terms of the result to be achieved which merely amounts to a statement of the underlying problem. The technical features necessary for achieving secure communication should be added.

- 5 The term "held (in encrypted form)" used in claim 16 is vague and unclear and leaves the reader in doubt as to the meaning of the technical feature to which it refers, thereby rendering the definition of the subject-matter of said claim unclear (Art. 6 PCT).

One way to overcome the objection would have been to replace "held" by "stored".

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB00/00495

- 6 Apparently claim 1 should read "a method of protecting from modification a computer apparatus comprising (...)".
- 7 The features of the claims 1-21 are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).